Universidade de Aveiro
2014
Departamento de Engenharia Mecânica

José Manuel Oliveira Carmo

Sistema de Gestão e Controlo de Acessos no Setor Hoteleiro

Universidade de Aveiro
2014

Departamento de Engenharia Mecânica

José Manuel Oliveira Carmo

Sistemas de Gestão e Controlo de Acessos no Setor Hoteleiro

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Automação Industrial, realizada sob orientação científica do Professor Doutor José Paulo Oliveira Santos, Professor auxiliar do Departamento de Engenharia Mecânica da Universidade de Aveiro.

O júri / The jury

Presidente / President	**Professor Doutor Pedro Nicolau Faria da Fonseca** Professor auxiliar da Universidade de Aveiro
Vogais / Commitee	**Professor Doutor Joaquim José Borges Gouveia** Professor Catedrático Convidado Aposentado da Universidade de Aveiro
	Professor Doutor José Paulo Oliveira Santos Professor auxiliar da Universidade de Aveiro (orientador)

Agradecimentos

Em primeiro lugar, agradeço aos meus pais, pelo apoio e dedicação incondicionais e, às minhas irmãs, por toda a ajuda e incentivo.
Agradeço à Adriana, pela ajuda e constante capacidade de motivação.
Expresso o meu agradecimento ao Professor Doutor José Paulo Santos (orientador), pelo apoio científico, pela capacidade critica e sugestiva durante o processo de desenvolvimento deste trabalho.
À Dra. Laurinda Seixas gostaria de expressar o meu agradecimento por todo o apoio e ajuda.
Por fim, gostaria ainda de agradecer a todos os meus colegas de laboratório, que, pela capacidade de cooperação e ajuda, possibilitaram um bom ambiente de aprendizagem e de trabalho.

Palavras-Chave

RFID, NFC, TCP, HTTP, Sistemas de Gestão, Base de Dados, PHP, HTML, Microcontroladores, Zigbee, XBee, Controlo, Serviços WEB, Turismo e Hotelaria.

Resumo

A presente dissertação descreve o desenvolvimento de um sistema de controlo e gestão de acessos, direcionado a entidades hoteleiras. Identificadas as características menos vantajosas e desajustadas das atuais soluções comerciais e académicas, o autor do trabalho propõe uma nova solução integrando num único sistema a capacidade de controlar e gerir acessos de pessoas tanto a espaços como a serviços. De modo a contornar dificuldades relacionadas com a incapacidade de acesso remoto e em tempo real à informação, a solução proposta neste trabalho visa um sistema de funcionamento *online* suportado por uma infraestrutura de comunicação globalizada, a qual possibilitará o acesso à informação independentemente das distâncias e localizações geográficas dos dispositivos de interface do sistema. A viabilidade do sistema desenvolvido depende de diversos fatores para além do seu básico funcionamento, questionando-se o controlo de acesso à informação e o nível invasivo do processo de identificação necessário à validação de acessos. Reunidas as condições, o desenvolvimento do sistema refere a estruturação de uma metodologia de identificação dos utilizadores com base numa tecnologia de suporte ajustada e que se demonstre eficiente, simples, segura e não invasiva para o utilizador. Analisadas diversas tecnologias de suporte à identificação, o sistema recorre à tecnologia RFID como responsável por permitir a identificação de utilizadores nos processos de validação de acessos. A interação com o sistema, relativamente a procedimentos de validação de acessos, é possível através de dispositivos de identificação RFID, concebidos ajustadamente com as funções necessárias a desempenhar. A monitorização e controlo de informação são efetuados com recurso a aplicações de interface gráfica concebidas para o efeito. Considerada a metodologia *online* do sistema, os requisitos de segurança definem-se mais rígidos, principalmente no que refere o acesso à informação. Por este motivo, é definida uma metodologia centrada no utilizador permitindo configurar individualmente a informação a que cada um pode aceder. Dadas as condições, o sistema exige a capacidade de identificar credivelmente cada um dos utilizadores, evitando o indevido acesso à informação através de falsas identificações. Por este motivo, o sistema utiliza um processo de identificação e autenticação baseado em credenciais (*Username* e *Password*) no acesso às aplicações de interface do sistema de informação.

Keywords RFID, NFC, TCP, HTTP, Management Systems, Database, PHP, HTML, Microcontrollers, Zigbee, XBee, Control, WEB Services, Tourism and Hostelry;

Abstract This thesis describes the development of a control and management access system targeted to hotel entities. Identified the least advantageous and misfits characteristics of the current commercial and academic solutions, the author of the paper proposes a new solution integrating into a single system the ability to control and manage access people to facilities and services. In order to circumvent difficulties related to the inability of remote access and real-time to the information, the solution proposed aims at an online system supported by a global communication infrastructure which will enable information access regardless of the interface devices´ geographic distances and localizations. The feasibility of the developed system depends on many factors beyond its basic operation, questioning the access control to information and the invasive level of identification process required for access validation. Gathered all conditions, the system development represents structuring a user´s identifying methodology based on a technology for this purpose and it is proven effective, simple, safe and non-invasive to the user. Analyzed various technologies to support the identification, the system uses the RFID technology as responsible for allowing the users´ identification in the access validation processes. The interaction with the system regarding access validation procedures is possible through RFID identification devices designed according to necessary functions. The monitoring and control of information is performed using the graphical user interfaces designed for this purpose. Considered the system´s online methodology, safety requirements are strictly defined, especially the access to information. For this reason, a user-centered methodology is defined which allows to configure the information that each user may access. With these conditions, the system requires a users´ credible identification process to prevent unauthorized access to information through fake Identifications. For this reason, the system uses an identification and authentication process based on credentials (username and password) to allow access to interface applications of information system.

Conteúdo

Capítulo 1 Introdução 3

1.1 Turismo em Portugal 3

1.1.1 Impacto económico 4

1.1.2 Serviços de alojamento 5

1.2 Enquadramento e Motivação 5

1.3 Problema 6

1.4 Objetivo 7

1.5 Organização da Dissertação 8

Capítulo 2 Controlo e Gestão de Acessos 11

2.1 Definição 11

2.2 Aplicação de Sistemas de Controlo e Gestão de Acessos 11

2.3 Tecnologias de Suporte à Identificação 13

2.3.1 Código de barras 13

2.3.2 Datamatrix 14

2.3.3 Cartões magnéticos 15

2.3.4 Cartões inteligentes 16

2.3.5 Processos biométricos 16

2.3.6 RFID 19

2.3.7 NFC 23

2.4 Tecnologias e Protocolos de Comunicação 24
2.4.1 Zigbee 24
2.4.2 Modbus 29
2.5 Soluções Académicas 33
2.5.1 Gestão e controlo de acessos 33
2.5.2 Novo sistema de rastreabilidade industrial 34
2.5.3 RFID na academia ATEC 35
2.6 Sistemas Comerciais 36
2.6.1 Telemax 37
2.6.2 Sursystems 38
2.6.3 Cifial 38
Capítulo 3 Conceção de uma Nova Solução 41
3.1 Arquitetura do Sistema de Dados 41
3.2 Tecnologia Suporte à Comunicação entre Dispositivos do Sistema 43
3.3 Tecnologia de Suporte à Identificação dos Utilizadores 44
3.4 Sistemas de Identificação e Validação de Acessos 46
3.4.1 Identificação e validação de acessos a serviços 46
3.4.2 Identificação e validação de acessos a espaços 47
3.5 Software de Interface com o Sistema de Informação 51
3.5.1 Interface do sistema de informação 51
3.5.2 Acesso personalizado ao sistema de informação 52
Capítulo 4 Implementação da Solução Proposta 55
4.1 Dispositivos 56
4.1.1 Equipamento de interação com etiquetas RFID 56
4.1.2 Etiquetas RFID 60
4.1.3 Dispositivo de leitura e escrita de etiquetas RFID 60
4.1.4 Dispositivos constituintes do sistema de validação de acessos a espaços 64

4.2 Software 78
4.2.1 Scripts 78
4.2.2 Aplicações de interação com o sistema de informação 79
4.3 Base de Dados 98
4.4 Servidor do Sistema 101
Conclusão 103
Bibliografia 105
A1 – Mensagens de leitura e escrita de etiquetas RFID. 115
A2 – Metodologias de comunicação I2C 117
A3 – Memória de dados de etiquetas RFID Mifare 119
A4 – Dispositivo de leitura e escrita de etiquetas RFID 121
A5 - Dispositivo de identificação para acesso a espaços 123
A6 - Módulo central de validação de acesso a espaços 125
A7 – Rede de comunicação Zigbee 127

Lista de Figuras

Figura 1.1: diagrama de interação do sistema a desenvolver (fonte própria)..... 7
Figura 2.1: abertura por código PIN (6)..... 12
Figura 2.2: relógio de ponto biométrico (7)..... 13
Figura 2.3: código de barras de acordo com a norma EAN-13 (9)..... 13
Figura 2.4: datamatrix (11)..... 14
Figura 2.5: cartão com banda magnética (12)..... 15
Figura 2.6: cartão inteligente (14)..... 16
Figura 2.7: cartão SIM (15)..... 16
Figura 2.8: leitor de impressão digital (16)..... 17
Figura 2.9: reconhecimento facial (17)..... 17
Figura 2.10: posicionamento das veias da mão (17)..... 18
Figura 2.11: análise da íris (19)..... 18
Figura 2.12: etiqueta RFID passiva (22)..... 20
Figura 2.13: etiqueta RFID ativa (23)..... 20
Figura 2.14: etiquetas RFID passivas (26)..... 22
Figura 2.15: pagamento com recurso a NFC (27)..... 23
Figura 2.16: comparativo entre tecnologias de comunicação sem fios (31)..... 25
Figura 2.17: topologias de rede Zigbee (33)(adaptada)..... 26
Figura 2.18: diagrama funcional do algoritmo CSMA/CA (34)..... 27
Figura 2.19: comunicação com mensagens Beacon inativas e ativas (32)..... 28
Figura 2.20: cenário de aplicação e interação entre sistemas (35)..... 29
Figura 2.21: Modbus segundo modelo OSI (37)..... 30
Figura 2.22: estrutura genérica de uma mensagem Modbus (37)..... 30

Figura 2.23: código das funções definidas pelo protocolo Modbus (37) 31
Figura 2.24: estrutura das mensagens Modbus RTU (38) 32
Figura 2.25: estrutura da mensagem Modbus ASCII (38) 32
Figura 2.26: acesso à plataforma WEBGPACS (39) 34
Figura 2.27: constituição do sistema de rastreabilidade industrial (24) 35
Figura 2.28: constituição da solução proposta (40) 36
Figura 2.29: dispositivo de validação de acesso (41) 37
Figura 2.30: sistema Sursystems (42)(adaptada) 38
Figura 2.31: constituição do sistema - funcionamento online (43) 39
Figura 3.1: arquiteturas de sistemas (44)(adaptada) 42
Figura 3.2: arquitetura prevista para o sistema (fonte própria) 43
Figura 3.3: sistema de validação de permissões de acesso a serviços (f.p) 47
Figura 3.4: sistema baseado numa rede RS485 e com recurso a um computador (f.p) 48
Figura 3.5: sistema baseado em dispositivos de comunicação direta com o servidor (f.p) 49
Figura 3.6: sistema baseado num dispositivo central de comunicação com o servidor (f.p) 50
Figura 3.7: utilizador do sistema (f.p) 54
Figura 4.1: cenário Funcional do sistema (fonte própria) 55
Figura 4.2: equipamento de Interação com etiquetas RFID Mifare (46)(adaptada) 57
Figura 4.3: equipamento de Interação com etiquetas RFID e NFC (48)(adaptada) 57
Figura 4.4: módulo de interação com etiquetas RFID (f.p) 58
Figura 4.5: exemplo de etiquetas RFID Mifare (tipo Cartão) (48)(adaptada) 60
Figura 4.6: cenário de utilização do dispositivo (f.p) 60
Figura 4.7: dispositivo de leitura e escrita de etiquetas RFID (f.p) 61
Figura 4.8: estrutura das mensagens enviadas do computador para o dispositivo (f.p) 62
Figura 4.9: estrutura das mensagens de resposta do dispositivo (f.p) 62
Figura 4.10: diagrama de comunicação entre o computador e o dispositivo (f.p) 63
Figura 4.11: cenário funcional dos dispositivos do sistema (f.p) 64
Figura 4.12: Módulos XBee (52) 65
Figura 4.13: MOD-ZIGBEE-UEXT (53) 66
Figura 4.14: cenário funcional do dispositivo (f.p) 68
Figura 4.15: dispositivo de identificação para acesso a espaço (f.p) 69
Figura 4.16: estrutura da mensagem de validação enviada pelo dispositivo (f.p) 70
Figura 4.17: estrutura da mensagem de resposta à validação do acesso (f.p) 70

Figura 4.18: diagrama de comunicação do dispositivo (f.p) 72
Figura 4.19: cenário funcional do dispositivo (f.p)..... 72
Figura 4.20: módulo central de validação de acesso a espaços (f.p) 73
Figura 4.21: conversor RS-232 to TCP/IP (Ethernet e Wi-fi) (58) 74
Figura 4.22: diagrama de comunicação do módulo (f.p) 74
Figura 4.23: interface Web de configuração do equipamento (58)..... 76
Figura 4.24: Mod-RS485 Olimex (59) 77
Figura 4.25: interface genérica de Login (f.p) 80
Figura 4.26: interface de pesquisa das duas funcionalidades (f.p)..... 81
Figura 4.27: interface de registo de credenciais (f.p) 81
Figura 4.28: interface da aplicação para utilizadores de estatuto “Super Administrador” (f.p) 82
igura 4.29: interface da aplicação para utilizadores de estatuto “Administrador” (f.p)..... 83
Figura 4.30: interface da aplicação administrador de serviços (f.p)..... 84
Figura 4.31: interface da aplicação administrador de espaços (f.p)..... 85
Figura 4.32: interface da aplicação administrador de entidades (f.p)..... 86
Figura 4.33: interface de gestão de contas e de etiquetas de utilizador (f.p) 87
Figura 4.34: interface da aplicação gestor de serviços (f.p)..... 90
Figura 4.35: interface de consulta dos registos de serviços prestados (f.p)..... 91
Figura 4.36: interface de consulta dos registos de atribuições de acesso a serviços (f.p) 92
Figura 4.37: interface de parametrização da consulta (f.p)..... 94
Figura 4.38: interface da aplicação gestor de espaços (f.p)..... 95
Figura 4.39 interface de consulta das atribuições de acesso a espaços efetuadas (f.p) 96
Figura 4.40: interface consulta das validações de acesso a espaços efetuadas (f.p) 97
Figura 4.41: interface de parametrização da consulta (f.p)..... 98
Figura 4.42: dados necessários armazenar e relação entre eles (f.p)..... 99
Figura 4.43: constituição e diagrama relacional UML da base de dados (f.p) 100
Figura 4.44: servidor do sistema (f.p) 101
Figura A1.1: interação para escrita e leitura de etiquetas RFID Mifare (49) 115
Figura A2.1: diagramas de comunicação I2C referentes às duas metodologias (49) 117
Figura A3.1: organização da memória de dados de etiquetas RFID Mifare (65) 119
Figura A4.1: esquema elétrico do dispositivo de leitura e escrita de etiquetas RFID (f.p).....121
Figura A5.1: esquema elétrico do dispositivo de identificação para acesso a espaços (f.p) 123
Figura A6.1: esquema elétrico módulo central de validação de acesso a espaços (f.p).....125

Figura A7.1: sistema exemplo que recorre a equipamentos de comunicação sem fios (f.p) 128
Figura A7.2: sistema exemplo de controlo e aquisição (f.p) 128
Figura A7.3: MOD-ZIGBEE-UEXT (53) 129
Figura A7.4: interfaces disponíveis no equipamento (53) (adaptada) 129
Figura A7.5: conexão ficha UEXT (66) (adaptada) 130
Figura A7.6: envio de carater entre dois computadores (f.p) 130
Figura A7.7: função ProcessUART (f.p) 132
Figura A7.8: código responsável pela execução da função ProcessUART (f.p) 132
Figura A7.9: código para envio de um caracter para o dispositivo coordenador (f.p) 133
Figura A7.10: exemplo de leitura do *buffer* de receção e envio para a UART (f.p) 133
Figura A7.11: estrutura da mensagem em modo *broadcast* (f.p) 138
Figura A7.12: estrutura da mensagem em modo *unicast* (f.p) 138
Figura A7.13: exemplo de funcionamento em modo *broadcast* (f.p) 138
Figura A7.14: exemplo de funcionamento em modo u*nicast* (f.p) 139
Figura A7.15: estrutura da mensagem a enviar (f.p) 140
Figura A7.16: funcionalidade de controlo e aquisição (f.p) 141
Figura A7.17: estrutura da mensagem recebida (f.p) 142
Figura A7.18: diagrama de interação da funcionalidade de controlo e aquisição (f.p) 142

Lista de Gráficos

Gráfico 1.1: registo de turistas nacionais e internacionais nos últimos cinco anos (1) (2) 3
Gráfico 1.2: receitas angariadas pelo turismo internacional nos últimos cinco anos (3) (4) 4
Gráfico 1.3: distribuição das Estadias em Portugal no ano 2013 (5) 5

Lista de Quadros

Quadro 3.1: características das arquiteturas (44)(adaptado) 42
Quadro 3.2: características de tecnologias de comunicação globalizadas (24)(adaptado) 44
Quadro 3.3: características das tecnologias de suporte à identificação (24) (39)(adaptado) 45

Glossário

AC *Alternate Current*

ADC *Analog-to-Digital Converter*

ADSL *Asymmetric Digital Subscriber Line*

AES *Advanced Encryption Standard*

AP *Access Point*

ASCII *American Standard Code for Information Interchange*

CR *Carriage Return*

CRC *Cyclic Redundancy Check*

CSMA/CA *Carrier Sense Multiple Access with Collision Avoidance*

CSMA/CD *Carrier Sense Multiple Access with Collision Detection*

CTS *Clear To Send*

DC *Direct Current*

DHCP *Dynamic Host Configuration Protocol*

EAN *European Article Number*

EEPROM *Electrically-Erasable Programmable Read-Only Memory*

EIA *Electronic Industries Alliance*

GSM *Global System for Mobile Communications*

HTML *Hypertext Markup Language*

HTTP *Hypertext Transfer Protocol*

I2C *Inter-Integrated Circuit*

ICSP *In Circuit Serial Programming*

IEC *International Electrotechnical Commission*

IEEE *Institute of Electrical and Electronics Engineers*

IP *Internet Protocol*

ISO *International Organization for Standardization*

Kbps *Kilobit Per Second*

LF *Line Feed*

LRC *Longitudinal Redundancy Check*

MAC *Media Access Control*

MD5 *Message Digest 5*

NFC *Near Field Communication*

OBDC *Open Database Connectivity*

OSI *Open Systems Interconnection*

PCB *Printed Circuit Board*

PIN *Personal Identification Number*

PHP *Hypertext Preprocessor*

PLC *Programmable Logic Controller*

RF *Radio Frequency*

RFID *Radio Frequency Identification*

RTS *Request To Send*

RTU *Remote Terminal Unit*

RX *Receiver*

SCL *Serial Clock*

SDA *Serial Data Signal*

SMS *Short Message Service*

SPI *Serial Peripheral Interface*

TCP *Transmission Control Protocol*

TTL *Transistor-Transistor Logic*

TX *Transmitter*

UART *Universal Asynchronous Receiver/Transmitter*

UDP *User Datagram Protocol*

UEXT *Universal Extension*

UML *Unified Modeling Language*

USB *Universal Serial Bus*

UTP *Unshielded Twisted Pair*

Capítulo 1 Introdução

1.1 Turismo em Portugal

O turismo afirma-se como um importante setor para a economia portuguesa, no entanto a conturbada situação económica dos últimos anos pode ter contribuído para variações menos positivas neste mercado específico. Dado o seu potencial para o país, deve ser compromisso a sua preservação e evolução. A excelência de serviços pode representar uma condição-chave para um comportamento positivo do setor em questão.

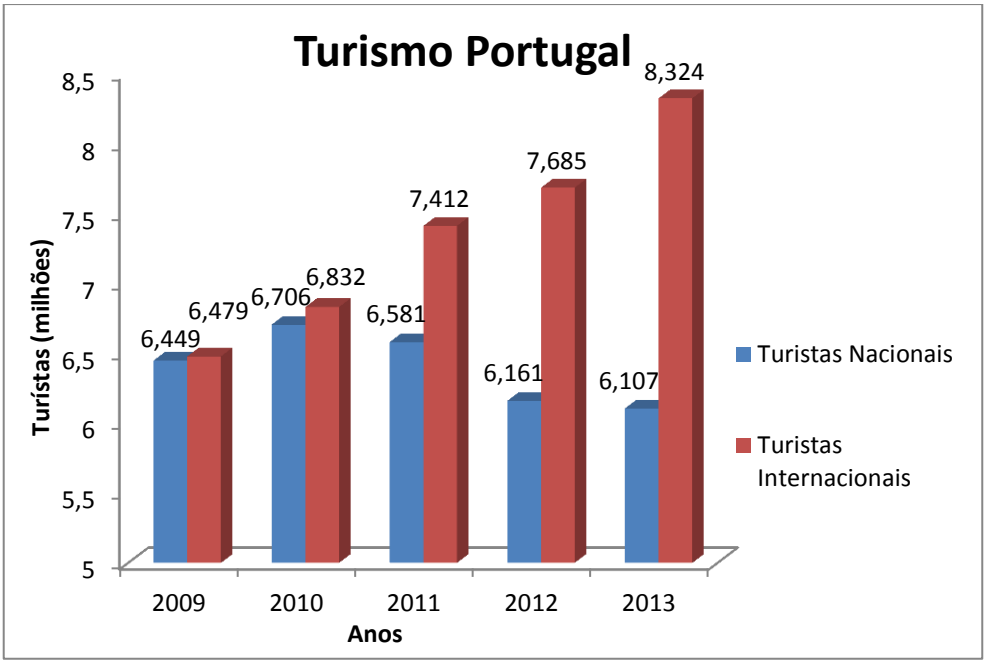


Gráfico 1.1: registo de turistas nacionais e internacionais nos últimos cinco anos (1) (2)

Nos últimos anos verificou-se uma variação na afluência ao turismo em Portugal: os marcadores referentes ao turismo nacional demonstram uma ligeira regressão porém os referentes ao turismo internacional revelam uma evolução de maior impacto (gráfico 1.1), traduzindo-se atualmente numa evolução positiva do setor.

De acordo com os dados estatísticos apresentados pelo ministério da economia, Portugal em 2013 registou através das unidades hoteleiras 14,4 milhões de hóspedes, dos quais, 8,3 milhões foram estrangeiros (2). Com uma população total de 10,53 milhões de habitantes, Portugal albergou, no ano de 2013, um número de turistas internacionais, correspondente a 78,8% da sua população total.

1.1.1 Impacto económico

Ainda de acordo com os dados do ministério da economia, em 2013, o setor em questão gerou cerca de 9,25 mil milhões de euros em receitas através do turismo internacional (3) e a previsão efetuada aponta para que a evolução registada nos últimos cinco anos (gráfico 1.2) continue nos seguintes.

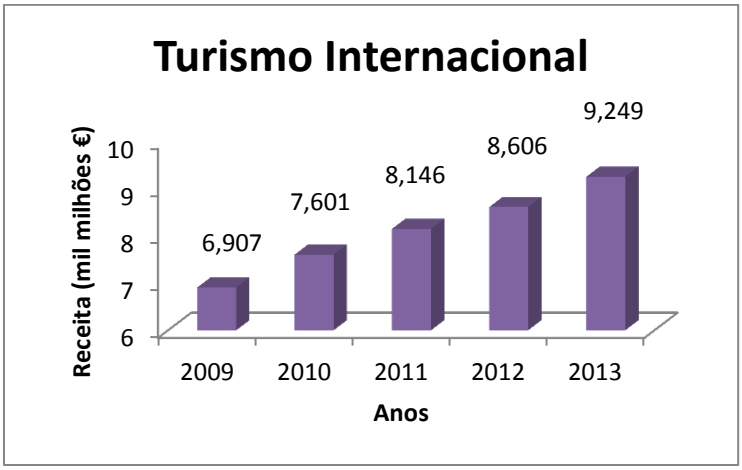


Gráfico 1.2: receitas angariadas pelo turismo internacional nos últimos cinco anos (3) (4)

Com uma evolução positiva para a economia, atualmente o crescimento das receitas do turismo internacional situa-se na ordem dos 7,5% por ano, traduzindo-se num consumo total no território económico na ordem dos 16 mil milhões de euros. Considerando o Produto Interno Bruto (PIB) nacional atual na ordem dos 165 mil milhões de euros, o setor representa atualmente uma fração próxima dos 10%, valor este que salienta claramente o impacto deste setor na economia.

1.1.2 Serviços de alojamento

O mercado do turismo é constituído por diversos serviços, mas são os referentes a alojamento que se destacam pela importância admitida no funcionamento de todo o sistema. Esta sua relevância justifica-se pela inclusão indispensável destes serviços na quase totalidade dos pacotes turísticos comercializados. Admitindo este importante papel para o setor, é necessário entender as modalidades o setor hoteleiro integra bem como estas se distribuem face à adesão do mercado. Apesar da diversidade de tipologias admitidas pelo setor de alojamento, em Portugal, aproximadamente 83% dos turistas recorrem a serviços de alojamento prestados por entidades hoteleiras, tal como demonstra o gráfico 1.3.

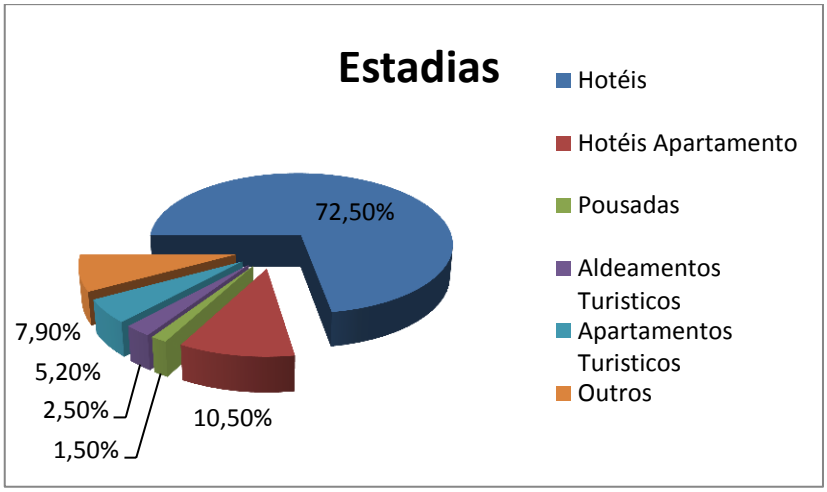


Gráfico 1.3: distribuição das Estadias em Portugal no ano 2013 (5)

De acordo com as estatísticas apresentadas pelo ministério da economia, no ano 2013 a distribuição dos serviços de estadia em hotéis (5) foi a seguinte:

- Hotéis 5 Estrelas: 12,3%
- Hotéis 4 Estrelas: 32%
- Hotéis 3 Estrelas: 18,6%
- Outros: 9,6%

1.2 Enquadramento e Motivação

De entre os diversos serviços turísticos, os de alojamento destacam-se nos estabelecimentos hoteleiros. Sendo o mercado de alojamento dominado por estes, a competitividade gerada promove a capacidade de distinção no mercado onde se integram.

Atualmente, estabelecimentos deste tipo procuram desenvolver e consolidar serviços periféricos de excelência como estratégia de diferenciação no mercado. A sustentabilidade destes serviços depende de diversos fatores, de entre os quais, a afluência, que só por si depende de um correto enquadramento deles na infraestrutura global e a capacidade de apresentar preços vantajosos relativamente a outros possíveis prestadores. Apesar destes serviços angariarem destaque para toda a infraestrutura, a sua rentabilidade não é desconsiderada, sendo esta um fator crítico para a sua continuidade.

A rentabilidade de um sistema depende da eficiência da sua gestão, da capacidade de simplificação e de otimização de mecanismos de recolha e tratamento de informação referente. A integração de cada um destes mecanismos num único, que possibilite por um lado o tratamento global de toda a informação referente à infraestrutura e, por outro, o tratamento diferenciado de cada serviço, pode representar uma mais-valia relevante pelo retorno de uma consistente percentagem acrescida na rentabilidade da infraestrutura. Considerando ainda a possível simplificação na execução de processos, através da automatização destes, de igual modo, resultados relevantes podem ser retornados.

O desenvolvimento de um sistema de gestão e controlo de dados, ajustado às necessidades do setor em questão, possibilitará um retorno positivo, tanto pela melhorada capacidade de gestão dos dados bem como, pela facilidade de acesso aos serviços prestada ao consumidor.

1.3 Problema

No que refere à gestão de acessos a espaços físicos, atualmente, alguns estabelecimentos implementam sistemas de suporte eletrónico para controlar e gerir este tipo de acesso, no entanto, estes apresentam na sua maioria limitações funcionais. Os sistemas atualmente aplicados possibilitam, na sua maioria, somente a gestão de acessos a espaços físicos em modo *offline*, isto é, não é possível em "tempo real" obter informações sobre os acessos até então efetuados, sendo posteriormente necessário efetuar uma recolha dessa informação junto dos equipamentos de identificação e autenticação, quando o sistema o possibilita. No mercado, surgem recentemente sistemas que possibilitam a recolha de informação referente a acessos em modo *online,* porém estes apresentam uma estrutura de funcionamento limitada, cuja resposta define-se no controlo de um conjunto de dados referentes a acessos a espaços de distribuição reduzida.

Para além das limitações descritas, os atuais sistemas impossibilitam a integração de informação referente a serviços periféricos. Apesar de existirem variadas soluções no mercado como resposta a problemas de gestão de informação, muitas limitações funcionais mantêm-se, dado não se encontrarem concebidas de acordo com todas as especificações relevantes.

1.4 Objetivo

Com recurso a tecnologias de identificação eletrónicas existentes, pretende-se desenvolver um sistema capaz de adquirir, monitorizar e controlar variáveis referentes a acessos efetuados e respetivas atribuições de permissão.

Particularmente nos estabelecimentos hoteleiros, pretende-se desenvolver um sistema que possibilite o controlo de acessos a espaços físicos e serviços, assim como permita o armazenamento e a gestão de toda essa informação (figura 1.1).

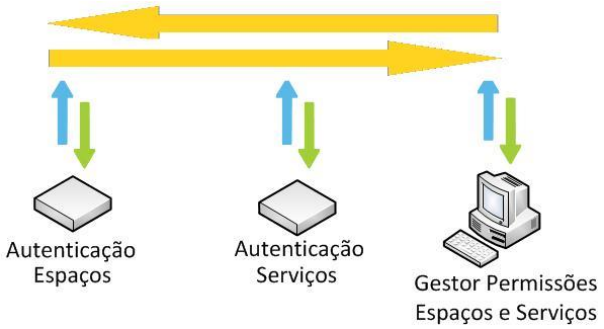


Figura 1.1: diagrama de interação do sistema a desenvolver (fonte própria)

Uma vez que o sistema deverá reunir a capacidade de controlo e gestão de acessos a serviços e espaços físicos, referentes a diversas entidades, é necessário que os dispositivos constituintes do sistema admitam capacidade de comunicação remota entre eles possibilitando o acesso à informação necessária em "tempo real" e independente da localização geográfica de cada dispositivo constituinte do sistema. O conjunto de informação disponibilizado deverá depender da prévia autorização de acesso à informação efetuada para cada utilizador do sistema.

1.5 Organização da Dissertação

A presente dissertação encontra-se organizada em cinco capítulos (incluindo o atual e a conclusão) e sete anexos. O capítulo atual descreve a relevância do setor turístico em Portugal, especificando a contribuição do mercado de alojamento. Com base nesta análise, o autor descreve também neste capítulo o enquadramento e a motivação desta dissertação. É enunciado ainda neste capítulo o problema que o autor propõe atenuar e o objetivo que o trabalho deverá alcançar.

O segundo capítulo apresenta o estado da arte relativamente ao controlo e à gestão de acessos, sendo iniciado por uma pequena definição e uma síntese das aplicações de sistemas deste tipo. Neste capítulo são enunciadas as tecnologias de suporte à identificação mais comuns e as tecnologias e protocolos de comunicação em destaque na solução desenvolvida neste trabalho. São ainda descritas resumidamente algumas soluções académicas e sistemas atualmente comercializados.

Com base no objetivo descrito no capítulo 1, o terceiro capítulo apresenta a estrutura e os conceitos genéricos da solução desenvolvida neste trabalho. É abordado neste capítulo a seleção da arquitetura do sistema de informação, da tecnologia de comunicação entre dispositivos, da tecnologia de suporte à identificação dos utilizadores e da plataforma de interface dos utilizadores com o sistema. Ainda neste capítulo são estruturados os dispositivos que são necessários desenvolver.

O quarto capítulo descreve a implementação do sistema, abordando descritivamente os dispositivos desenvolvidos e o *software* tanto de processamento como de interface. Neste capítulo é também apresentada a estrutura e a relação da base de dados bem como, são definidos os requisitos do servidor do sistema.

No quinto capítulo são apresentadas as conclusões do trabalho, referenciando a análise funcional do sistema e aspetos de melhoria a considerar numa futura continuidade de desenvolvimento do mesmo.

Relativamente aos anexos, no primeiro é apresentado um diagrama de interação que exemplifica as mensagens necessárias transmitir entre o microcontrolador e o equipamento de interação com etiquetas RFID, de modo a possibilitar a escrita e leitura de dados em etiquetas RFID Mifare. No segundo, também com recurso a diagramas de interação, são demonstradas as duas metodologias de comunicação possíveis entre o microcontrolador e o equipamento de interação com etiquetas RFID, recorrendo a uma comunicação I2C. O terceiro anexo apresenta

esquematicamente a estrutura da memória de dados de uma etiqueta RFID Mifare. Os três anexos seguintes apresentam os esquemas elétricos dos dispositivos concebidos, sendo no quarto anexo apresentado o esquema do dispositivo de leitura e escrita de etiquetas RFID, no quinto apresentado o esquema do dispositivo de identificação para acesso a espaços e no sexto apresentado o esquema do módulo central de validação de acesso a espaços.

Por fim, no sétimo anexo é descrito o trabalho de configuração (programação) de equipamentos MOD-ZIGBEE-UEXT, de modo a possibilitar a transmissão de dados entre equipamentos com recurso a uma comunicação sem fios RF Zigbee.

Capítulo 2 Controlo e Gestão de Acessos

2.1 Definição

Individualizando cada um dos termos constituintes, controlo refere a capacidade de monitorizar e alterar uma ou diversas variáveis de um ou mais processos. Aplicado a sistemas, a alteração de variáveis pode ser condicionada pelos dados monitorizados (sistema realimentado) ou independentemente destes (sistema aberto).

Relativamente à gestão, esta define-se como a capacidade de organização e interpretação de informação. Da relação das informações interpretadas, quando referentes a um sistema, é possível validar os procedimentos funcionais, possibilitando posteriormente, a redefinição dos mesmos quando falhas ou desajustes forem verificados. Sucintamente, controlo prevê a execução processual, enquanto gestão prevê a análise dos processos.

A junção dos dois termos, aplicados a sistemas de acessos, define integralmente a capacidade de atuação e rastreamento processual de um ou vários sistemas de validação, registando todos os acontecimentos.

2.2 Aplicação de Sistemas de Controlo e Gestão de Acessos

A procura por ferramentas que melhorem a capacidade de identificar e eliminar quaisquer desperdícios recursivos torna-se a cada dia mais exaustiva, admitindo a tecnologia um papel fundamental nesta questão. Os recursos tecnológicos têm permitido, para além da execução processual facilitada, automatizada e mais eficiente, a definição específica de intervalos de erros e suas probabilidades.

Sistemas de controlo e gestão de acessos, pela sua abrangência, podem integrar diversas aplicações, contudo, todas elas admitem em comum a criteriosa capacidade de recolha e registo de informações referentes a rastreamento pessoal e a atuações sistémicas.

Uma das mais relevantes aplicações, a qual fundamenta parte deste trabalho, é a de validação de permissões de acesso de pessoas a espaços (figura 2.1).

Figura 2.1: abertura por código PIN (6)

Estes sistemas possibilitam a fácil atribuição e remoção de permissões de acesso a espaços sendo que, pelo registo e organização da informação associada, facilmente são verificadas as ocorrências de acessos a um determinado espaço. Esta capacidade possibilita verificar se acessos indevidos ocorreram ou, pelo contrário, se acessos que deveriam ter ocorrido não se verificam como, por exemplo, acessos de pessoal de manutenção.

Uma outra aplicação, que recorre a este tipo de sistemas, é demonstrada pela figura 2.2 e representa um sistema de registo de entrada e saída de funcionários numa entidade: relógio de ponto.

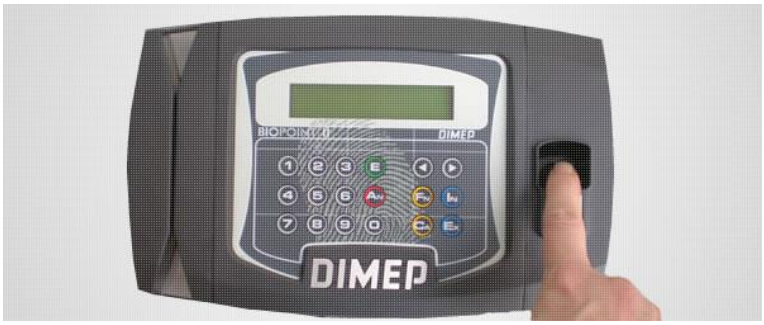


Figura 2.2: relógio de ponto biométrico (7)

Com um sistema deste tipo, é possível reunir informações que permitem o controlo das horas de serviço de um funcionário, diária, semanal, mensal e anualmente. Sistema requerido para controlo da rentabilidade associada às horas de serviço do pessoal contratado.

2.3 Tecnologias de Suporte à Identificação

2.3.1 Código de barras

O conceito da tecnologia código de barras nasce em 1932 com o intuito de possibilitar a identificação de produtos no setor logístico, contudo o primeiro sistema de identificação desta tecnologia só foi concebido em 1948 (8). A tecnologia de identificação por código de barras consiste na representação gráfica de códigos numéricos e alfanuméricos tal como demonstra a figura 2.3. A codificação do valor é efetuada pela variação da largura e do espaçamento das barras.

Figura 2.3: código de barras de acordo com a norma EAN-13 (9)

Embora o conceito seja comum, a diversidade de requisitos na identificação impôs a necessidade de se normalizarem simbologias tanto para representações numéricas como alfanuméricas. Algumas das simbologias normalizadas (9) são:

Alfanuméricos:

- Código 128;
- GS1-128 (antigo EAN-128);
- Código 39;
- Código 93;
- LOGMARS: Igual ao código 93 com especificação E.U.A.

Numéricos:

- Codabar;
- Código 11;
- EAN-13;
- EAN-8;
- 2 de 5 Industrial;
- 2 de 5 Standard;
- 2 de 5 Intercalado;
- MSI;
- Plessey;
- PostNet;
- UPC-A;
- UPC-E.

2.3.2 Datamatrix

Esta tecnologia, tal como a código de barras, representa graficamente um valor numérico ou alfanumérico. A necessidade de integrar mais informação num único código gerou a procura por novas soluções, sendo esta concebida em 1994 (10). A sua utilização primordial foi na indústria automóvel.

Figura 2.4: datamatrix (11)

Como demonstra a figura 2.4, esta codificação é efetuada em duas dimensões, daí a capacidade de armazenamento de informação ser superior. A interpretação pode ser feita com recurso a telemóveis que integrem câmara fotográfica, a qual possibilita a captação da informação necessária para posterior descodificação, com recurso a uma aplicação para o efeito. A captação pode ser efetuada em qualquer ângulo que possibilite a captação da imagem referente ao código, uma vez que, através dos localizadores de posicionamento, é possível orientar corretamente o processo de descodificação.

Pela facilidade de codificação e maior capacidade de informação, esta codificação é atualmente utilizada para diversas funcionalidades, tais como acesso facilitado a plataformas web, a endereços e contactos. Esta tecnologia pode ser utilizada na própria identificação logística.

2.3.3 Cartões magnéticos

Os cartões magnéticos, tal como o nome pressupõe, consiste numa tecnologia que recorre a uma banda magnética como meio de guardar dados, permitindo múltiplas escritas e leituras. Esta banda é acoplada em cartões (figura 2.5) daí a denominação atribuída à tecnologia de identificação.

Figura 2.5: cartão com banda magnética (12)

A escrita é efetuada por um dispositivo que possibilita a alteração da polarização magnética ao longo da banda, com recurso ao campo magnético que gera e direciona. A leitura é efetuada pelo processo contrário, ou seja, por um dispositivo que possibilita a perceção da orientação magnética ao longo da banda.

Podendo ser escritos dados em diversas áreas da banda, foram definidas normas que possibilitem estabelecer especificações de armazenamento de dados na mesma (13). Atualmente cada banda magnética possibilita o armazenamento em três áreas: superior, inferior e intermédia.

2.3.4 Cartões inteligentes

Cartões inteligentes são cartões que integram um circuito de processamento, composto por um microcontrolador e memória de dados tal como as etiquetas RFID, contudo o estabelecimento de comunicação com estes dispositivos é efetuado por uma ligação física. Os cartões em questão, como demonstra a figura 2.6, apresentam um conjunto de contactos elétricos que possibilitam a interação com o dispositivo.

Figura 2.6: cartão inteligente (14)

Embora a sua integração seja atualmente realizada em diversos cartões, como cartões bancários, a sua principal aplicação é nas comunicações móveis sendo esta tecnologia usada nos cartões SIM (figura 2.7).

Figura 2.7: cartão SIM (15)

2.3.5 Processos biométricos

Processos biométricos referem tecnologias que possibilitam a identificação de seres vivos com base em características físicas únicas, cuja probabilidade de dupla ocorrência seja praticamente nula. Atualmente estão comprovadas um conjunto de características como sendo teoricamente exclusivas a cada ser vivo. Recorrendo a dispositivos tecnológicos atuais e a

algoritmos de processamento, é possível recolher, interpretar e associar os dados respetivos a cada ser vivo, possibilitando a sua identificação.

2.3.5.1 Impressão digital

A impressão digital consiste na representação gráfica definida pelas elevações da pele das pontas dos dedos. A captação gráfica pode ser efetuada com recurso a sensores concebidos para o efeito (figura 2.8), sendo a sua interpretação efetuada posteriormente por algoritmos específicos.

Figura 2.8: leitor de impressão digital (16)

2.3.5.2 Reconhecimento facial

O reconhecimento facial é um processo de identificação que recorre a um conjunto de processos de medição entre pontos pré-definidos e captados na face. O seu procedimento é complexo dada a reunião e intersecção de uma diversidade de dados necessários para possibilitar o reconhecimento correto.

Figura 2.9: reconhecimento facial (17)

Como demonstra a figura 2.9, o processo consiste em relacionar matematicamente determinados pontos faciais, recolhendo dados como distâncias métricas e angulares.

2.3.5.3 Posicionamento das veias das mãos

Esta tecnologia consiste em recolher uma imagem por radiação local, em que sejam identificáveis as veias de uma das mãos (figura 2.10).

Figura 2.10: posicionamento das veias da mão (17)

A partir do padrão de disposição é possível reunir informações suficientes para a identificação do respetivo indivíduo.

2.3.5.4 Padrão da íris

A tecnologia de identificação por análise do padrão da íris (figura 2.11) é atualmente a que representa a maior fiabilidade de todas as tecnologias de identificação por processos biométricos, estimando-se que a probabilidade de ocorrência de igualdade entre Íris de dois indivíduos seja $1/10^{72}$ (18).

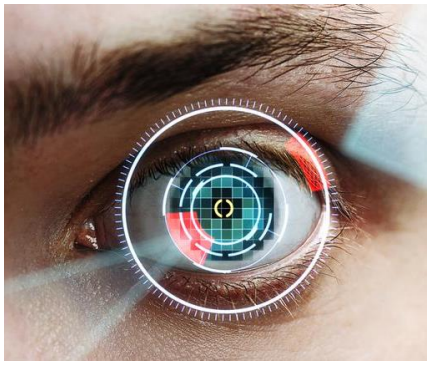


Figura 2.11: análise da íris (19)

2.3.6 RFID

A tecnologia RFID visa possibilitar a identificação de pessoas e objetos recorrendo a comunicação por radiofrequência com dispositivos a eles associados ou acoplados.

O conceito base desta tecnologia surge no seguimento da segunda guerra mundial pela necessária identificação dos aviões inimigos (20). Desenvolvido por *Watson-Watt*, o sistema inicial consistia num recetor-transmissor acoplado aos aviões que, após receber uma mensagem pré definida e devidamente modulada emitida em terra, respondia com uma mensagem de retorno que seria recebida e possibilitaria a identificação do dispositivo, identificando o respetivo avião.

O desenvolvimento tecnológico continuou em torno desta tecnologia e, em 1973, foram patenteadas as primeiras etiquetas RFID. A primeira patente refere-se a uma etiqueta ativa (alimentação própria) com memória regravável, sendo que a segunda refere-se a uma etiqueta passiva (alimentação induzida), cujo funcionamento foi testado no controlo de abertura de uma porta sem recorrer a uma chave mecânica de acesso (20). Desde então, bastantes progressos têm sido feitos mantendo-se inalterável o princípio base. Atualmente, a tecnologia define-se pela diversidade de dispositivos suportados, aplicações e protocolos de comunicação.

Sistemas de identificação RFID são constituídos por etiquetas (*transponders*) e leitores (21). O leitor é o dispositivo que irá interrogar a etiqueta quando esta estiver dentro do seu campo de interação procedendo, deste modo, ao estabelecimento de comunicação, possibilitando a identificação da respetiva etiqueta RFID. As etiquetas podem conter um microcontrolador e memória, que, dependendo da arquitetura pode ser integrada no microcontrolador, e por um circuito de transmissão de radiofrequência. A definição de uma etiqueta depende dos tipos de características que respeitam.

2.3.6.1 Tipologia de alimentação

No que refere a tipologia de alimentação, as etiquetas podem admitir três distintas definições: passivas, ativas e semi-ativas.

Etiquetas Passivas

As etiquetas do tipo passivas (figura 2.12) não integram qualquer fonte de energia acoplada, sendo a energia necessária à alimentação do circuito transferida pelo leitor.

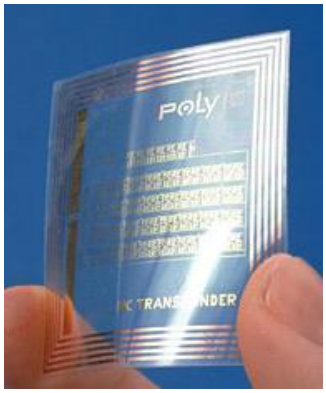


Figura 2.12: etiqueta RFID passiva (22)

Recorrendo à mesma antena do transmissor RF, é possível obter energia elétrica do campo magnético gerado pelo leitor. Dada esta característica, o estabelecimento de comunicação é normalmente dependente da distância entre os dispositivos.

Etiquetas Ativas

Etiquetas ativas (figura 2.13), contrariamente às do tipo passivo, integram uma fonte de alimentação não sendo necessário requisitar potência ao dispositivo leitor.

Figura 2.13: etiqueta RFID ativa (23)

Tanto a alimentação do circuito integrado, como o sinal de rádio, recorrem à energia disponibilizada pela fonte de energia acoplada. A difusão do sinal emitido pode não depender do leitor, o que possibilita a comunicação entre este e a etiqueta sem que sejam cumpridos rígidas limitações de distância entre eles. A capacidade de processamento destas é normalmente superior à das anteriores, uma vez que podem decorrer processos sem que para isso seja necessária a sua proximidade com um leitor.

Etiquetas Semi-ativas

Etiquetas semi-ativas, também denominadas semi-passivas, apresentam-se como um tipo hibrido, uma vez que admitem características de ambas as anteriores descritas.

Este tipo de etiquetas integra, tal como as ativas, uma fonte de alimentação acoplada, contudo esta é somente responsável por fornecer energia ao microcontrolador. A difusão do sinal mantem dependência do sinal emitido por um dispositivo leitor. A distância entre os dispositivos, normalmente, assume valores intermédios relativamente às duas anteriores.

2.3.6.2 Armazenamento de dados

No que refere ao armazenamento de dados, as etiquetas admitem três definições possíveis: apenas leitura, leitura e escrita e *write once read many* (WORM) (24). Tal como a designação o indica, as etiquetas do tipo apenas leitura não possibilitam a escrita de qualquer dado. Estas somente possibilitam a sua identificação e recolha de dados não configuráveis.

As etiquetas de leitura e escrita teoricamente possibilitam configurações ilimitadas de informação armazenada, bem como o acesso a esta.

As etiquetas do tipo WORM possibilitam uma única configuração dos dados, não podendo estes ser posteriormente reconfigurados. A leitura dos dados não assume limitações.

2.3.6.3 Normalização

Dado que a tecnologia admite uma diversidade de dispositivos e aplicações foram necessárias normalizações que possibilitaram definir características para dispositivos e processos de funcionamento. Atualmente diversas normas encontram-se definidas para a tecnologia RFID sendo as normas abertas divididas em quatro grupos (25):

- Normas tecnológicas: definem características de interface entre leitores e etiquetas (Ex: frequências de modulação - ISO/IEC 18000)
- Normas envolvendo informação: definem padrões da informação (Ex: definição do ID da etiqueta - ISO 15963)
- Normas de conformidade: definem metodologias de verificação de conformidade de dispositivos com uma dada norma (Ex: teste no desempenho de dispositivos RFID - ISO 18046)

- Normas aplicativas: definem critérios de utilização das etiquetas relativamente à aplicação em questão (Ex: utilização de etiquetas de identificação automática de contentores de carga - ISO 10374)

Além das normas que se inserem nos quatro grupos apresentados, existem normas não definidas de acordo com os quatro tipos descritos dado, tratarem-se de normas proprietárias, ou seja, desenvolvidas por organizações que definem padrões exclusivos. Um exemplo de uma organização responsável por desenvolver normas proprietárias é a NXP Semiconductors. Esta organização é a responsável pela normalização de etiquetas Mifare. Apesar de proprietárias, muitas normas deste tipo são compatíveis com normas de acesso livre. A normalização proprietária enunciada é um exemplo desta situação uma vez que, admite total compatibilidade com a norma ISO/IEC 14443 A. A norma internacional ISO/IEC 14443 define duas metodologias protocolares, sendo elas denominadas do seguinte modo: ISO/IEC 14443 A e ISO/IEC 14443 B. Ambas definem frequências de modulação e taxas de transmissão idênticas: 13,56MHz e 106kbit/s, mas referentemente a metodologias de modulação e codificação são distintas (25).

2.3.6.4 Formatos físicos de etiquetas passivas RFID

Dada a simplicidade do circuito integrado das etiquetas RFID passivas relativamente a outros dispositivos, atualmente a sua inserção em objetos de diversos formatos físicos é possível facilmente. Pela diversidade de aplicações recorrentes a esta tecnologia, o mercado disponibiliza etiquetas RFID integradas em vários objetos (figura 2.14) como cartões, etiquetas autocolantes, crachás, pulseiras, chaves de automóveis entre outros.

Figura 2.14: etiquetas RFID passivas (26)

2.3.7 NFC

A tecnologia de comunicação NFC foi desenvolvida com base no conceito da tecnologia RFID sendo esta concebida como forma de possibilitar a transmissão de informação entre dispositivos próximos sem recurso a ligações físicas. Com recurso a esta tecnologia, é também possível interagir com etiquetas RFID que cumpram os requisitos de comunicação.

Dadas as possíveis funcionalidades e características, atualmente alguns modelos de *smartphones* integram esta tecnologia como interface de comunicação. Com recurso a aplicativos específicos é possível a estes dispositivos recolher e inserir informações em etiquetas RFID bem como transferir dados entre dispositivos. Pela capacidade de transferência de dados entre dispositivos, atualmente existem aplicações que recorrem a esta interface e possibilitam a utilização de um *smartphone* para efetuar pagamentos em substituição da utilização de cartões bancários. A figura 2.15 demonstra um procedimento de pagamento, utilizando um *smartphone* que integra esta tecnologia.

Figura 2.15: pagamento com recurso a NFC (27)

A tecnologia respeita duas das normas da tecnologia RFID, ou seja, ISO/IEC 14443 e ISO/IEC 18000-3. Estas normas definem os protocolos de transmissão e as condições físicas necessárias ao estabelecimento de comunicação entre os dispositivos. Definido pelas normas, a comunicação entre dispositivos é possível, quando a distância entre eles não ultrapassa os 4cm, sendo a frequência de modulação dos sinais de dados efetuada a 13,56MHz (28).

2.4 Tecnologias e Protocolos de Comunicação

2.4.1 Zigbee

A tecnologia de comunicação Zigbee foi desenvolvida pela Zigbee Alliance (29), organização fundada em 2002 com intuito de apresentar um novo sistema de comunicação sem fios. Em 2004 foram reunidas todas as especificações funcionais para a tecnologia, no entanto, só passados dois anos, em 2006, foi provado o seu funcionamento com o apresentação dos primeiros dispositivos aptos a comunicarem segundo as especificações desta tecnologia. O seu desenvolvimento foi justificado principalmente pela carência de tecnologias de comunicação sem fios ajustadas às necessidades de sistemas de aquisição e controlo. Uma vez constituídos por sensores e atuadores, a capacidade destes comunicarem internamente no sistema, sem que para tal fossem requeridas ligações físicas entre eles, constituía uma vantagem significante para a viabilidade dos mesmos. Embora existissem tecnologias de comunicação sem fios como, por exemplo, Bluetooth e Wi-Fi, as suas características não apresentavam o melhor ajuste para com sistemas deste tipo principalmente no refere as exigências energéticas. Sendo parte dos dispositivos constituintes alimentados por pequenas baterias, a implementação de uma tecnologia de comunicação de elevada exigência energética inviabilizaria este processo de alimentação. Deste modo, a tecnologia ZigBee surge admitindo como característica primordial o baixo consumo energético. Associado a este, encontra-se a impossibilidade de transmissão de elevados fluxos de informação, contudo, para os sistemas que originaram o seu desenvolvimento, esta característica não define qualquer desajuste, dado que não são esperadas grandes transmissões de informação.

2.4.1.1 Características

A tecnologia ZigBee foi desenvolvida respeitando as especificações definidas pela norma IEEE 802.15.4 (30), sendo possível estabelecer 27 canais diferentes de comunicação, cuja distribuição é efetuada pelas seguintes três faixas de frequência de modulação:

- 2,4GHz – 16 canais
- 915MHz – 10 canais
- 868MHz – 1 canal

A faixa de modulação 2,4GHz é aceite globalmente, contudo, as duas restantes são utilizadas em duas áreas geograficamente distintas, isto é, a faixa dos 915MHz é utilizada na

América enquanto a faixa dos 868MHz é utilizada na Europa. Ainda referente a cada uma das faixas, o fluxo de dados máximo suportado varia de acordo com cada uma delas em função das larguras de banda definidas para cada um dos respetivos canais de comunicação. Relativamente aos canais de comunicação modulados na faixa dos 2,4GHz, estes admitem uma taxa máxima de transmissão igual 250Kbps, enquanto os canais modulados na faixa de frequência de 915MHz suportam uma transmissão máxima de 40Kbps. O canal de comunicação modulado a 868MHz suporta uma taxa de transmissão máxima igual a 20kbps. Relativamente a outras tecnologias de comunicação sem fios, como demonstra a figura 2.16, esta apresenta a menor taxa de transmissão de dados.

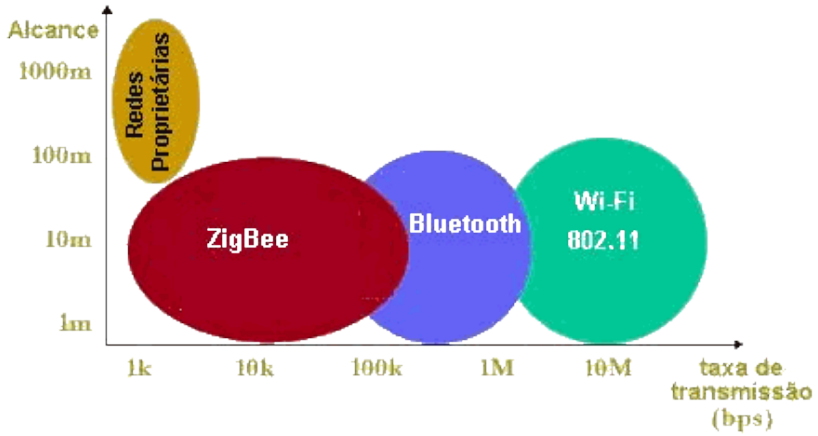


Figura 2.16: comparativo entre tecnologias de comunicação sem fios (31)

Relativamente aos dispositivos definidos pela tecnologia (32), estes reúnem-se em dois grupos, ou seja, dispositivos de funções globais e dispositivos de funções reduzidas. O primeiro grupo reúne dois dispositivos, isto é, coordenadores e *routers*. O segundo refere um único tipo, ou seja, dispositivos terminais. Dependendo dos dispositivos utilizados e da dispersão física, a rede de comunicação pode assumir uma das três topologias representadas esquematicamente pela figura 2.17.

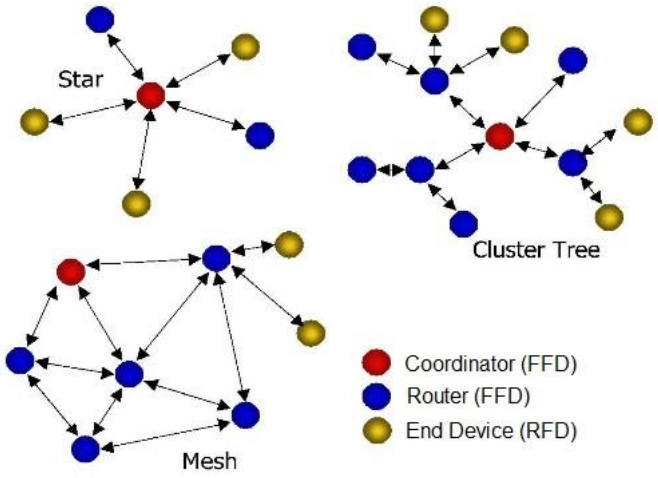


Figura 2.17: topologias de rede Zigbee (33)(adaptada)

Como se verifica na figura 2.17, por cada rede é necessário um dispositivo coordenador. Este dispositivo é o responsável por estabelecer a rede e, deste modo, somente um é admissível e indispensável por rede ZigBee. Relativamente aos *routers* e dispositivos terminais, ambos podem ser opcionais dependendo da topologia e das funcionalidades previstas a efetuar. A diferença entre eles verifica-se no modo de operação, ou seja, os dispositivos terminais, ao contrário dos *routers*, não permitem associar dispositivos à rede através de si. Pelo facto de somente atenderem mensagens a si destinadas, encontram-se em estado *sleep* a maior parte do tempo, saindo deste modo só quando necessitam de comunicar ou receber informação. Caso se pretenda que a topologia da rede seja estrela, dispositivos *router* podem ser dispensados. Por outro lado, para possibilitar que a rede admita uma topologia diferente de estrela, os *routers* são obrigatoriamente necessários, podendo, dependendo das funcionalidades, dispensar-se dispositivos terminais. Os dispositivos terminais, pelas suas características (principalmente o facto de maioritariamente se encontrarem em modo *sleep*) são os que menos recursos energéticos requerem para o funcionamento.

Uma vez que qualquer dispositivo da rede emite dados, é necessário garantir que as mensagens emitidas são recebidas corretamente sem que nenhuma perturbação possa influenciar os dados. Uma perturbação significante pode ser gerada caso dois dispositivos transmitam simultaneamente originando uma colisão das mensagens, impossibilitando a correta receção das mesmas pelo respetivo dispositivo destino. Como forma de controlar as mensagens de dados na rede, a tecnologia implementa um algoritmo de controlo de acesso ao meio denominado (32) *CSMA/CA*. Este algoritmo estabelece que cada dispositivo antes de emitir uma

mensagem de dados deverá emitir uma mensagem de verificação do meio. Caso ocorra alguma colisão ou o meio se encontre ocupado por outro dispositivo, nenhuma mensagem de confirmação será enviada, pelo que o dispositivo deverá assumir indisponibilidade do meio. Deste modo, aguardará um tempo aleatório e voltará a verificar disponibilidade. Caso o meio se encontre disponível, após o dispositivo emitir a mensagem de verificação, uma mensagem será recebida, informando que o meio estará livre para efetuar a transmissão. A figura 2.18 apresenta um fluxograma que esquematiza o funcionamento descrito.

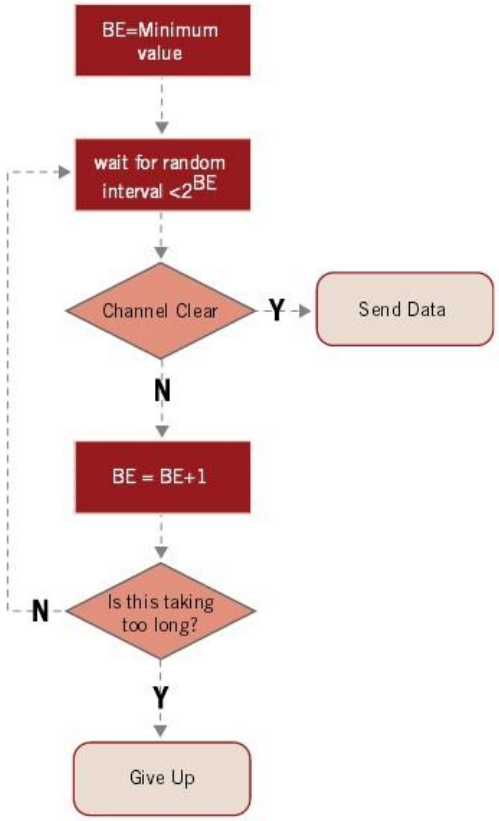


Figura 2.18: diagrama funcional do algoritmo CSMA/CA (34)

Como forma de possibilitar uma melhor sincronização dos dispositivos conectados à rede, ao coordenador é possível atribuir a capacidade de estabelecer intervalos de tempo dedicados à emissão de dados dos dispositivos. Estes intervalos podem ser subdivididos possibilitando definir um intervalo específico para a conexão de novos dispositivos na rede. Esta característica de funcionamento é designada por *beacon network communication*. A figura 2.19 apresenta dois diagramas de interação refentes à comunicação na rede com ou sem recurso a esta característica.

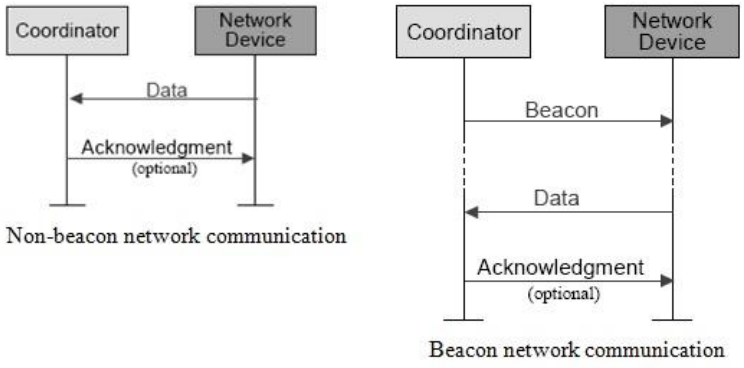


Figura 2.19: comunicação com mensagens Beacon inativas e ativas (32)

A ativação desta característica funcional permite ao coordenador obter melhores ferramentas de controlo da rede, reduzindo latências, uma vez que, a ocorrência de determinados processos é efetuada organizadamente dentro de intervalos de tempo específicos.

O endereçamento físico dos dispositivos (MAC) é efetuado em oito bytes, o que possibilita a distinção de $18460x10^{15}$ dispositivos. Sendo as redes endereçadas (PAN ID) por dois bytes é possível distinguir 65535 redes ZigBee (32). Dado que o endereçamento Zigbee dos dispositivos numa rede é efetuado com recurso a um *short address* (dois bytes), cada rede da tecnologia suporte um máximo teórico de 65536 dispositivos. Por motivos de segurança, a tecnologia possibilita a criptografia 128 AES. Dada a potência prevista dos sinais de radiofrequência (1mW), a distância máxima entre dispositivos sem obstáculos de atenuação considerável é aproximadamente 100m.

Dadas as atuais aplicações da tecnologia de comunicação Zigbee, um novo dispositivo foi requerido de forma a possibilitar a interface entre a rede de comunicação Zigbee e outras redes, tais como a rede Internet. O dispositivo é designado como *gateway*.

2.4.1.2 Aplicações

Inicialmente desenvolvida como resposta às necessidades de comunicação de sistemas de domótica, atualmente é utilizada numa diversidade de sistemas bem como em interligações entre eles.

Com o avanço tecnológico dos últimos anos, a atual diversidade de dispositivos inteligentes constitui pequenos sistemas tecnológicos, pelo que, a restrita capacidade de comunicação interna em cada um deles não responde às necessidades, sendo requerido para além da comunicação interna nos sistemas, que estes possam capacidade de comunicação remota entre eles. Acompanhando as necessidades do mercado, à tecnologia Zigbee foram

adicionadas características funcionais que permitem que esta se torne cada vez mais eficiente nos sistemas que a integram, firmando uma melhor viabilidade no mercado. Atualmente as redes de comunicação desta tecnologia facilmente interagem com outras redes da mesma ou de diferentes tecnologias (ver figura 2.20)

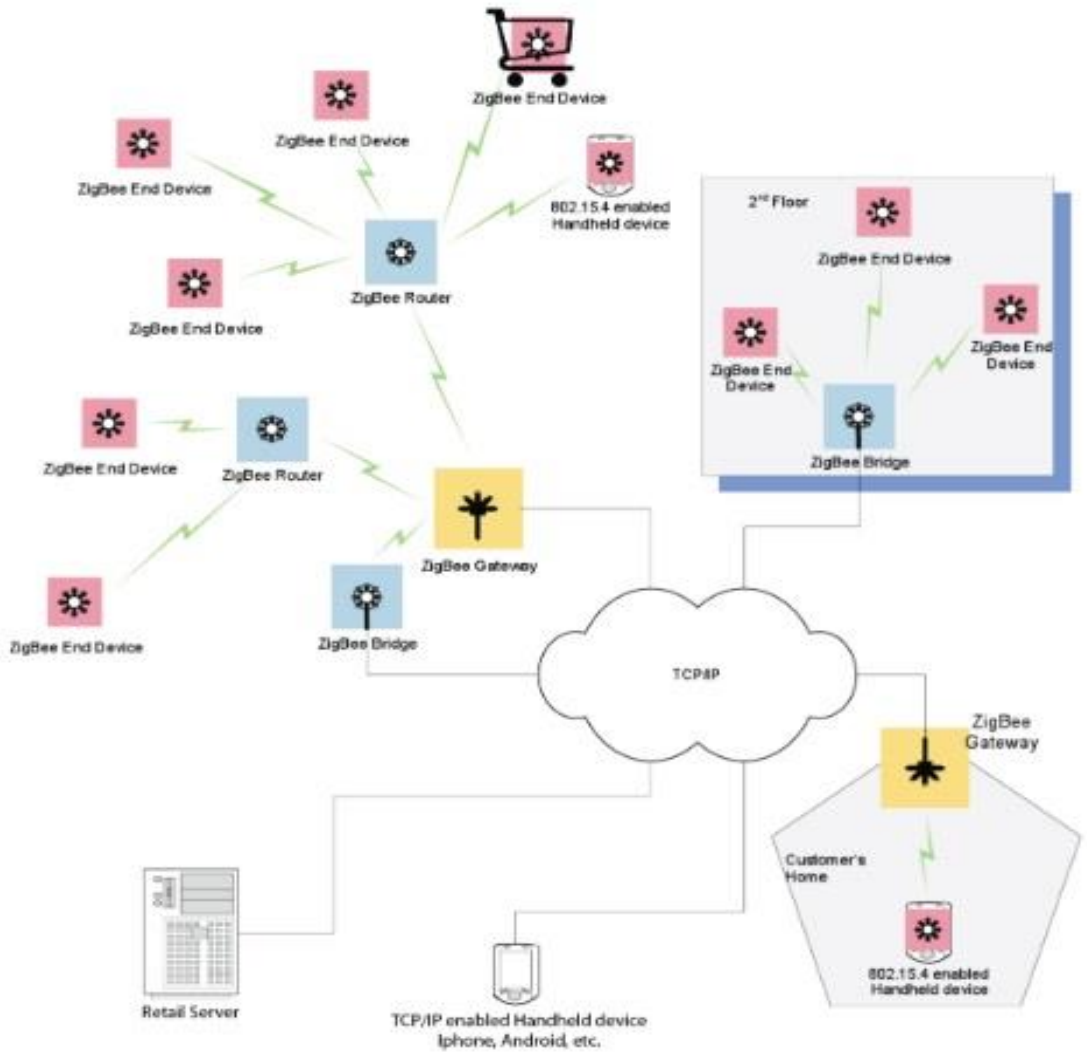


Figura 2.20: cenário de aplicação e interação entre sistemas (35)

2.4.2 Modbus

Modbus é um protocolo de comunicação desenvolvido pela Modicon, em 1979. Em 2004, os direitos foram concedidos à organização Modbus tornando a utilização deste protocolo livre e sem custos de licenciamento (36). Este protocolo define somente a estrutura de mensagens,

sendo um protocolo segundo o modelo *OSI* pertencente à camada de aplicação. Como tal, este não define qualquer topologia de comunicação nem qualquer característica para o meio físico, podendo ser utilizado em diversas redes de comunicação, tais como Ethernet, EIA-232, EIA-485 e ainda redes sem fios e redes de fibra ótica (37). A figura 2.21 demonstra a relação do protocolo com diversas infraestruturas de comunicação segundo o modelo OSI.

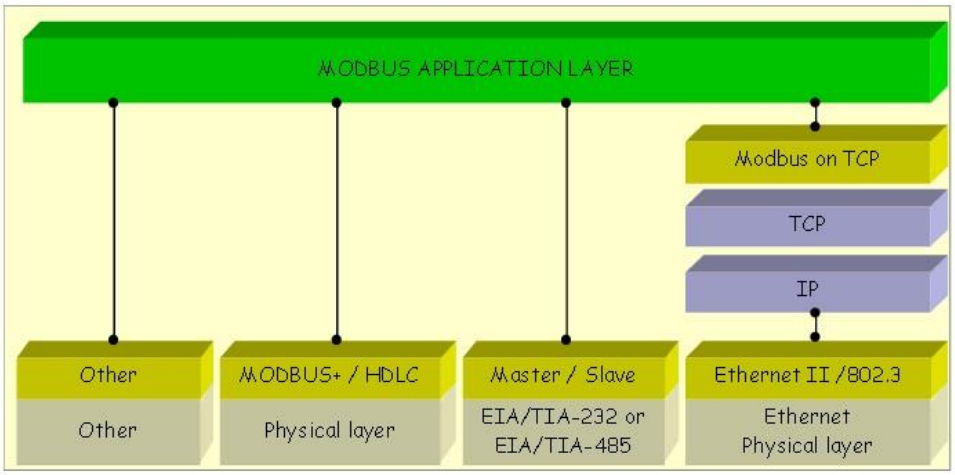


Figura 2.21: Modbus segundo modelo OSI (37)

O protocolo foi desenvolvido com o intuito de permitir a comunicação entre PLCs. Pela fácil e livre implementação, atualmente é um dos protocolos mais utilizadores em redes de autómatos de diversos fabricantes.

O protocolo define um diálogo do tipo *Master/Slave*, isto é, somente o dispositivo master poderá enviar mensagens em qualquer instante, sendo que os dispositivos *Slave* só o poderão fazer em resposta a um pedido prévio do *Master*. Como tal, o master é sempre o dispositivo responsável por iniciar o diálogo, impossibilitando a comunicação direta entre dois dispositivos *Slave*. As mensagens genericamente são compostas por um campo endereço, preenchido com o endereço do dispositivo *Slave* com o qual pretende estabelecer diálogo, o campo função que permite indicar o procedimento a efetuar pelo *Slave*, um campo de dados e um campo de validação da mensagem que possibilitará verificar se a mensagem recebida corresponde exatamente à mensagem emitida. A figura 2.22 demonstra a estrutura genérica das mensagens definida pelo protocolo.

Figura 2.22: estrutura genérica de uma mensagem Modbus (37)

Relativamente às funções, o protocolo define um conjunto de valores que referem procedimentos específicos. A figura 2.23 apresenta um quadro que relaciona os códigos da função com respetiva descrição.

				Function Codes			
				code	*Sub code*	*(hex)*	*Section*
Data Access	**Bit access**	Physical Discrete Inputs	Read Discrete Inputs	**02**		**02**	6.2
		Internal Bits Or Physical coils	Read Coils	**01**		**01**	6.1
			Write Single Coil	**05**		**05**	6.5
			Write Multiple Coils	**15**		**0F**	6.11
	16 bits access	Physical Input Registers	Read Input Register	**04**		**04**	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	**03**		**03**	6.3
			Write Single Register	**06**		**06**	6.6
			Write Multiple Registers	**16**		**10**	6.12
			Read/Write Multiple Registers	**23**		**17**	6.17
			Mask Write Register	**22**		**16**	6.16
			Read FIFO queue	**24**		**18**	6.18
	File record access		Read File record	**20**		**14**	6.14
			Write File record	**21**		**15**	6.15
Diagnostics			Read Exception status	**07**		**07**	6.7
			Diagnostic	**08**	**00-18,20**	**08**	6.8
			Get Com event counter	**11**		**OB**	6.9
			Get Com Event Log	**12**		**0C**	6.10
			Report Server ID	**17**		**11**	6.13
			Read device Identification	**43**	**14**	**2B**	6.21
Other			Encapsulated Interface Transport	**43**	**13,14**	**2B**	6.19
			CANopen General Reference	**43**	**13**	**2B**	6.20

Figura 2.23: código das funções definidas pelo protocolo Modbus (37)

Como é possível verificar, as funções estipuladas e reservadas pelo protocolo apresentam-se específicas a processos executados por autómatos, contudo existe um conjunto de valores de funções não utilizados que o podem ser, caso haja necessidade de definir determinados procedimentos em sistemas específicos.

De forma a possibilitar ajuste com uma maior diversidade de sistemas, o protocolo define duas estruturas distintas de mensagens, ou seja, mensagens tipo RTU e ASCII.

2.4.2.1 Mensagens RTU

Nas mensagens do tipo RTU, as representações dos dados são efetuadas diretamente com o valor hexadecimal respetivo. Deste modo, como é possível verificar pela figura 2.24, os campos endereço e função admitem um byte cada.

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1–T2–T3–T4	8 BITS	8 BITS	n x 8 BITS	16 BITS	T1–T2–T3–T4

Figura 2.24: estrutura das mensagens Modbus RTU (38)

O início da mensagem é assinalado pelo star bit do primeiro dado a enviar (endereço) uma vez que, não é definido nenhum caracter de início de mensagem. De igual modo, não é definido para esta tipologia de mensagem um caracter ou um conjunto de caracteres de terminação, pelo que, duas mensagens não podem ser sucessivamente enviadas dado que somente o início de uma seria detetado. Como forma de possibilitar a individualização de cada mensagem por qualquer dispositivo, entre o ultimo byte de uma mensagem enviada e o primeiro byte de uma mensagem sucessiva a enviar deve ser aguardado um tempo igual ou superior ao tempo necessário à transmissão de 3,5 bytes (38).

Relativamente ao valor de validação, nesta tipologia este pode admitir 65536 valores distintos (CRC 16). O valor deste campo é calculado segundo um algoritmo de complexa descrição.

2.4.2.2 Mensagens ASCII

As mensagens ASCII, contrariamente às mensagens RTU, admitem uma estrutura que integra caracteres de início e terminação. As mensagens são iniciadas pelo caracter ":" e terminadas pela sequência dos dois caracteres CR e LF (38). Como é possível verificar pela estrutura representada na figura 2.25, o campo endereço e o campo função são compostos por dois bytes.

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	n CHARS	2 CHARS	2 CHARS CR LF

Figura 2.25: estrutura da mensagem Modbus ASCII (38)

Embora não sendo percetível na totalidade, este tipo de mensagem requer dois bytes para representar um byte hexadecimal, ou seja, cada valor deve ser representado graficamente pelos caracteres ASCII (Ex: endereço 0x0F deverá ser representado por "0" seguido de "F"). Deste

modo, este tipo de mensagem perde eficiência face ao tipo RTU, uma vez que ambas admitem globalmente o mesmo tamanho máximo, contudo, neste tipo, cada valor representado requisita dois bytes enquanto o tipo RTU requisita somente um.

O valor LRC, tal como CRC é utilizado para possibilitar a verificação de erros na mensagem. Tal como qualquer campo, o valor em hexadecimal deste deverá ser representado pelos caracteres respetivos. O valor deste campo é calculado em função dos valores representados graficamente por caracteres ASCII e referentes aos campos endereço, função e dados. A soma em oito bits dos valores representados nestes campos mais o valor representado no campo LRC deverá ser igual a zero.

2.5 Soluções Académicas

O autor procura neste tópico apresentar resumidamente algumas soluções académicas propostas por outros autores. Através destas, o autor procurou recolher o máximo de informação referente aos sistemas preconcebidos, que de algum modo possam apresentar conceitos relevantes a atender no desenvolvimento de uma nova solução, tal como este trabalho o propõe.

2.5.1 Gestão e controlo de acessos

Dada a dificuldade de gerir e controlar acessos a espaços físicos, MOREIRA, Pedro (2008) propôs o desenvolvimento de uma aplicação que permitisse efetuar a gestão e o controlo de acessos (39), tendo ajustado o sistema para um cenário concreto, neste caso um campus universitário. Apesar de ser apresentado um estudo prévio de tecnologias para identificação e autenticação, o trabalho não propõe qualquer desenvolvimento neste sentido, dado que o autor do trabalho considera que o Hardware já se encontra definido e implementado. Deste modo, o objetivo concreto deste trabalho é o desenvolvimento de uma plataforma que possibilite interagir com o sistema e deste modo gerir toda a informação. De entre várias possibilidades para o desenvolvimento da interface, o autor seleciona uma página web. Esta escolha resulta principalmente pela facilidade de acesso que esta possibilita, uma vez que para o seu acesso nada mais que um WebBrowser será necessário estar instalado nos dispositivos que pretendam efetuar o acesso à interface. Dada a seleção, o trabalho refere então o desenvolvimento de uma página *web* com recurso às linguagens de programação que possibilitam interação do utilizador com o sistema (PHP) e a dinâmica local da página (Javascript). O armazenamento dos dados necessários para o correto funcionamento do sistema é efetuado por uma base de dados MySQL. A

plataforma desenvolvida neste trabalho é denominada pelo autor como WEBGPACS, sendo demonstrada a estrutura do sistema pela figura 2.26.

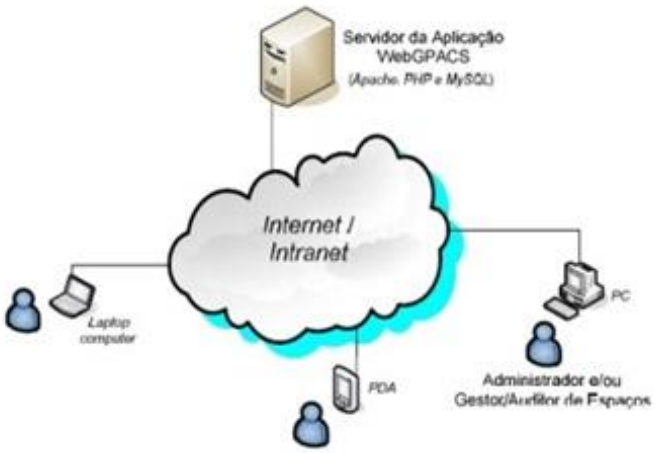


Figura 2.26: acesso à plataforma WEBGPACS (39)

A arquitetura do sistema prevê o funcionamento em modo *online*, dado que possibilita o acesso à informação remotamente e "tempo real", uma vez que o sistema de dados é centralizado num servidor *web*.

2.5.2 Novo sistema de rastreabilidade industrial

Como forma de identificação, ALMEIDA, João (2012) no seu trabalho de dissertação (24) seleciona a tecnologia RFID como forma de identificação no sistema de rastreabilidade industrial desenvolvido. Neste trabalho é apresentado um comparativo entre diferentes tecnologias que possibilitem a identificação, sendo a RFID a que demonstra o melhor conjunto de vantagens relevantes segundo o autor do trabalho. Apesar de a sua implementação poder ser relativamente mais complexa, a sua utilização é simplificada e o nível de segurança previsto é elevado. A imagem 2.27 ilustra a estrutura do sistema desenvolvido.

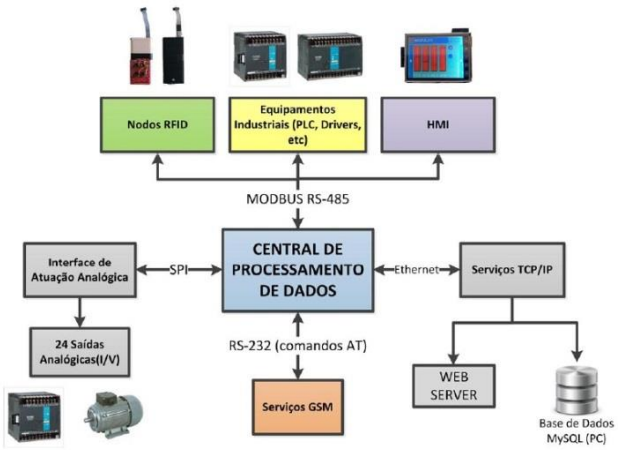


Figura 2.27: constituição do sistema de rastreabilidade industrial (24)

O sistema desenvolvido integra a possibilidade de gerir a informação dentro de uma infraestrutura industrial. Possibilita também a interação remota através de serviços GSM e ainda através da rede internet dado implementar, num microcontrolador, um servidor web.

2.5.3 RFID na academia ATEC

Com a perspetiva de conceber um sistema de controlo e gestão de acessos a espaços físicos, TEIXEIRA, Manuel (2008) no seu trabalho de dissertação (40) procurou estruturá-lo com recurso a dispositivos e *software* disponíveis no mercado. Inicialmente, o autor do trabalho apresenta um estudo sobre tipos de dispositivos RFID e o seu funcionamento, finalizando com um comparativo entre esta tecnologia e a tecnologia código de barras (tecnologia de identificação mais utilizada atualmente). Procura na proposta de solução apresentar um conjunto de sistemas, presentes atualmente no mercado, possíveis de implementar, selecionando no final do estudo aquele que possibilita somente identificação por etiquetas RFID (ver figura 2.28).

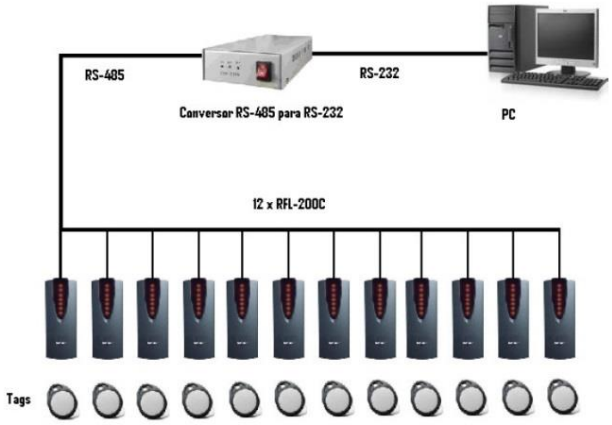


Figura 2.28: constituição da solução proposta (40)

Uma vez que o objetivo deste trabalho é estruturar um sistema que possibilite somente o controlo e gestão de acessos num único edifício (área reduzida), o acesso à informação fora das instalações não foi requisito sendo o centro de dados do sistema composto por um computador instalado no interior das instalações. Não sendo necessária uma infraestrutura de comunicação que possibilite o acesso remoto ao sistema, a rede de comunicação implementada para interligar todos os dispositivos constituintes é um barramento RS-485. O computador encontra-se conectado a esta rede de comunicação com recurso a um conversor RS-485-RS-232 dada a impossibilidade de conectar diretamente ao barramento RS-485, através das suas interfaces físicas de comunicação.

O *software* de gestão e controlo de acessos selecionado foi o *software* da Telemax para o efeito. Este deverá estar instalado no computador juntamente com os serviços de base de dados.

2.6 Sistemas Comerciais

Com o propósito de perceber as limitações na capacidade de gestão de acessos, o autor realizou um estudo de mercado com o intuito de verificar as soluções que este oferece na atualidade. De entre diversos sistemas encontrados, foram selecionados três que melhor se ajustam às aplicações destacas por este trabalho, sendo apresentadas para cada um deles as limitações associadas.

2.6.1 Telemax

A empresa Telemax apresenta um sistema de gestão e controlo de acessos para hotel (41). O sistema é composto por dispositivos de programação de etiquetas eletrónicas, etiquetas eletrónicas (cartão RFID Mifare), dispositivos de identificação e validação das etiquetas conectados às fechaduras (figura 2.29), dispositivos de recolha de dados e o *software* de gestão da informação referente ao sistema.

Figura 2.29: dispositivo de validação de acesso (41)

O sistema apresenta uma metodologia de funcionamento *offline*, isto é, não é possível obter informação de acessos em "tempo real", uma vez que, não existe qualquer sistema de comunicação que interligue os dispositivos e possibilite a transmissão de informação. Resumidamente, o funcionamento do sistema prevê a recolha manual de dados com recurso aos dispositivos para o efeito junto aos de identificação e validação. A etiqueta é programada, com recurso ao computador e ao dispositivo de programação de etiquetas, sendo esta responsável por armazenar a informação referente aos acessos permitidos. Posteriormente, e quando o procedimento de acesso ao espaço for efetuado, de acordo com a informação das etiquetas, os dispositivos de identificação processam os dados e retornam o resultado da validação, armazenando também estes, informação sobre as validações efetuadas. Quando uma etiqueta é programada, o *software* de gestão recolhe a informação referente. Para tornar possível gerir os acessos efetuados, os dados recolhidos pelos dispositivos previstos para o efeito são transferidos para o computador sendo recebidos pela aplicação de gestão. Somente após estes procedimentos a informação encontrar-se-á atualizada.

O fornecedor do sistema possibilita diferentes tipos de dispositivos de identificação e autenticação com o intuito de apresentar soluções de aplicação facilitadas, no entanto o sistema apresenta por um lado a limitação de somente possibilitar o controlo e gestão de acessos a espaços físicos. Por outro lado, a metodologia de funcionamento *offline* limita a capacidade de gestão pela necessária recolha manual de informação.

2.6.2 Sursystems

A empresa Sursystems disponibiliza o acesso a um sistema (42), o qual ao contrário do anterior, adota um funcionamento em modo *online*.

O sistema é composto pelos dispositivos de identificação, acoplados às fechaduras, dispositivos codificadores de etiquetas RFID, etiquetas RFID e o *software* de gestão hoteleira (figura 2.30).

Figura 2.30: sistema Sursystems (42)(adaptada)

O *software* não possibilita somente a gestão do sistema de acessos, integrando conjuntamente funcionalidades periféricas da gestão hoteleira. As fechaduras são alimentadas por baterias, não sendo requeridas fontes de alimentação junto às portas e a transmissão de dados, entre os dispositivos de identificação e o computador (dotado com o software de gestão) pode ser efetuada em "tempo real", através da rede Ethernet com recurso ao protocolo TCP/IP.

Apesar do sistema possibilitar a recolha de informação referente aos acessos em tempo real, apresenta a limitação da impossibilidade de integração de sistemas de controlo e gestão de serviços com base na mesma tecnologia de identificação. A integração de funcionalidades periféricas de gestão hoteleira num único *software* de gestão poderá em determinados cenários apresentar desajustes face às necessidades, comprometendo a rentabilidade do sistema.

2.6.3 Cifial

Ao contrário das soluções apresentadas anteriormente, a empresa Cifial apresenta um sistema de controlo e gestão de acessos para hotel (43) com duas metodologias de funcionamento respondendo com uma maior diversidade neste sentido.

Numa primeira abordagem, o sistema tal como os anteriores, pode ser constituído de forma a adotar um modo de funcionamento *offline*. De forma a combater as possíveis limitações de um sistema deste tipo, este pode ser reconfigurado e dotado com uma metodologia de funcionamento *online*. Se for definido com uma metodologia de funcionamento *offline*, o conjunto formado pelo dispositivo de identificação e a fechadura poderá ser alimentado com recurso a baterias, não sendo requerida qualquer fonte de alimentação junto às portas. Ainda para este modo de funcionamento, podem ser definidos cartões magnéticos e/ou etiquetas RFID como dispositivos identificadores. Caso a metodologia de funcionamento adotada seja *online*, o conjunto fechadura e dispositivo identificador é obrigatoriamente alimentado pela rede elétrica (230V AC) e é necessário conectar o conjunto à rede Ethernet com recurso a um cabo UTP. Neste modo de funcionamento, somente são possíveis etiquetas RFID como identificadores. A constituição do sistema com esta abordagem funcional é representada pela figura 2.31.

Figura 2.31: constituição do sistema - funcionamento online (43)

Contrariamente aos anteriores sistemas descritos, o sistema disponível pela Cifial (43) apresenta diversidade tanto a nível da metodologia de funcionamento como dos dispositivos constituintes, o que lhe atribui uma vantagem sobre os restantes. Embora se realce esta distinção pelas características anunciadas, detêm tal como os outros a limitação de impossibilidade de integração de um sistema de controlo e gestão de serviços.

Capítulo 3 Conceção de uma Nova Solução

Atendendo ao objetivo enunciado no capítulo 1, o trabalho propõe o desenvolvimento de um sistema de gestão e controlo de acessos constituído por dispositivos e interfaces computacionais. Sendo necessário o acesso à informação atualizada, a partir de qualquer dispositivo, é requisito fundamental que estes possam transmitir dados entre si, contudo, por questões de segurança, cada utilizador do sistema deverá somente ter acesso à informação que lhe foi previamente deferida autorização.

O funcionamento do sistema depende da capacidade de acesso à informação em "tempo real" e que esta possa ser acedida por qualquer dispositivo do sistema. Considerando que a área de dispersão dos dispositivos é indefinida, o acesso à informação depende de infraestruturas de comunicação globalizadas e de acesso tangível. O desenvolvimento de uma proposta de solução para o problema concreto requer inicialmente a definição da tecnologia de comunicação e da arquitetura do sistema, sendo posteriormente necessária a adaptação e conceção de dispositivos e *software,* que permitam na sua reunião uma dinâmica correta para o funcionamento integral do sistema.

3.1 Arquitetura do Sistema de Dados

Pelo necessário acesso à informação de qualquer dispositivo, o sistema impõe uma metodologia de acesso e armazenamento de dados remotos. Imposta esta necessidade, o sistema deve adotar uma arquitetura genérica que possibilite o melhor ajuste com as necessidades de interação entre dispositivos.

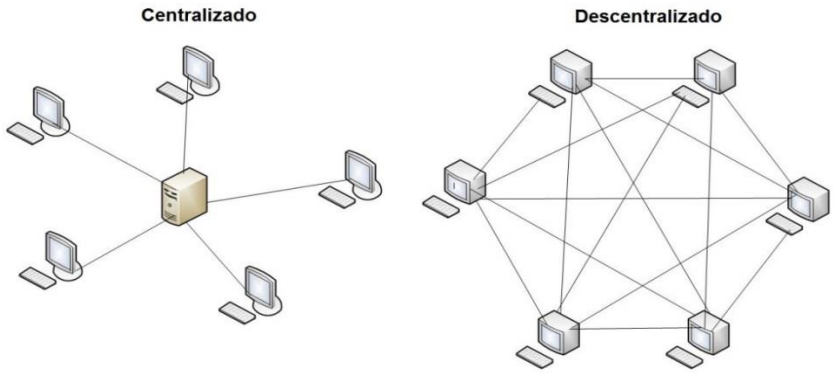


Figura 3.1: arquiteturas de sistemas (44)(adaptada)

Podendo o sistema assumir uma das arquiteturas exemplificadas na figura 3.1, foram abordadas e comparadas as características referentes a cada uma delas (quadro 3.1) com o propósito de selecionar a que demonstra o melhor ajuste face às necessidades.

Quadro 3.1: características das arquiteturas (44)(adaptado)

Arquitetura Centralizada	Arquitetura Descentralizada
• Cliente requisita e atualiza informação • Servidor armazena informação e envia-a ao cliente que a requisita • Falha do servidor corrompe o funcionamento do sistema • Falha de um cliente não é percetível aos restantes, não comprometendo o funcionamento do sistema • Fácil implementação de mecanismos de segurança (servidor) • A segurança do sistema não depende dos clientes • Atualização de dados fiável • Fácil controlo dos acessos à informação • Ajustada a sistemas de comunicação a longas distâncias	• Os dispositivos são simultaneamente Clientes e Servidores • A informação é armazenada pelos diversos dispositivos • Possível redundância de informação pela fragmentação associada • Falha de um dispositivo poderá impossibilitar o acesso a uma parte da informação, comprometendo o total funcionamento do sistema • Difícil controlo dos acessos à informação • Atualização de dados pode exigir um processo complexo e falível pela necessidade de atualização em vários pontos • A segurança do sistema depende da segurança dos clientes • Ajustada a sistemas de curta distância

Apesar da arquitetura centralizada depender totalmente do funcionamento de um único dispositivo (servidor), no que refere a segurança dos dados e a fiabilidade funcional do sistema, apresenta-se vantajosa relativamente à arquitetura descentralizada. Ainda são garantidas melhores características de segurança aos clientes, uma vez que os seus dispositivos numa arquitetura centralizada não necessitam admitir conexões para além das que estabelecem com o

servidor. Esta mesma característica constitui a vantagem do funcionamento do sistema ser totalmente independente do estado funcional de um dispositivo cliente.

Reunida informação referente ao comparativo entre as características correspondentes a cada tipo de arquitetura, o autor seleciona uma arquitetura centralizada para estrutura base do sistema (figura 3.2).

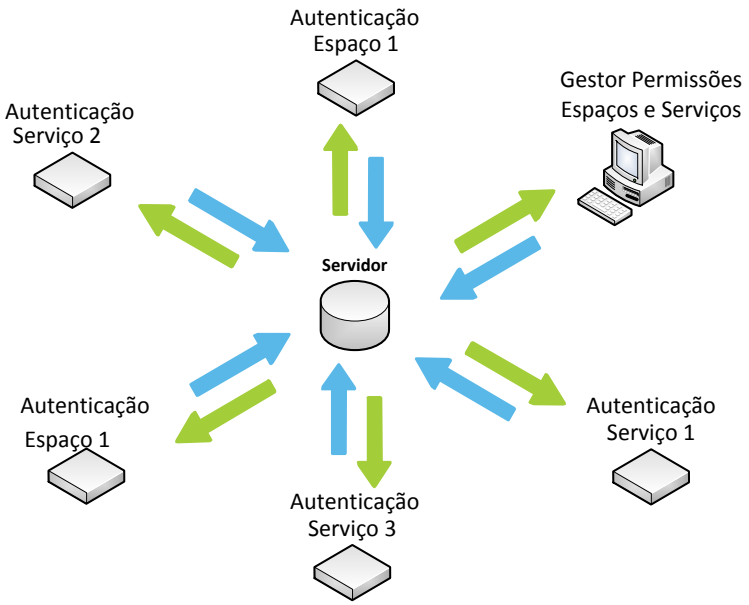


Figura 3.2: arquitetura prevista para o sistema (fonte própria)

3.2 Tecnologia Suporte à Comunicação entre Dispositivos do Sistema

Uma vez que o sistema será constituído por um número indefinido de dispositivos que necessitam aceder a informação global, é necessário garantir que estes se encontrem aptos a comunicarem numa mesma rede. Dada a prevista dispersão geográfica nas localizações dos dispositivos, o recurso a tecnologias de comunicação privadas não possibilitará o cumprimento das necessidades impostas, uma vez que as redes de comunicação deste tipo apresentam limitações no que refere as distâncias de cobertura.

Com estas condições, as únicas infraestruturas de comunicação que integram as características necessárias para o funcionamento do sistema, são as redes de comunicação globalizadas e que possibilitam integração tangível pelo sistema:

- Rede Internet: ADSL, 2G, 3G, 4G e outras;
- Serviços GSM-SMS.

Embora ambas as redes de comunicação possibilitem a transmissão de dados a longas distâncias, cada uma delas ajusta-se a determinadas funcionalidades, sendo que a seleção desta deverá ser efetuada de acordo com as características apresentadas no quadro 3.2 e referentes a cada uma delas.

Quadro 3.2: características de tecnologias de comunicação globalizadas (24)(adaptado)

Internet	GSM-SMS
• Acesso à rede possível por infraestruturas cabladas ou sem fios (curta e longa distância) • Ajustada à transmissão de mensagens entre dispositivos computacionais e com finalidades processuais. • Custos taxados de acordo com os dados transmitidos	• Acesso à rede através de dispositivos móveis (sem fios) • Transmissão de mensagens de texto cuja finalidade é interpretação direta do utilizador. • Custos taxados de acordo com as conexões efetuadas

Embora as mensagens de texto previstas pela tecnologia GSM, através de pacotes SMS possam sofrer posterior processamento computacional, a conexão dos dispositivos à rede respetiva implica a necessidade de dispositivos específicos de interface. Por outro lado, a rede *internet* ajusta-se diretamente com funcionalidades de comunicação entre dispositivos computacionais. Por este motivo, este tipo de dispositivos integram diversos modos de conexão às infraestruturas de comunicação desta tecnologia sem que sejam na maioria requeridos dispositivos extra.

Dado que o sistema prevê maioritariamente computadores como dispositivos constituintes, a seleção pela tecnologia GSM seria desajustada pelo que, o autor seleciona a **rede Internet** como a infraestrutura de comunicação apropriada às características previstas para o sistema.

3.3 Tecnologia de Suporte à Identificação dos Utilizadores

Sendo a utilidade do sistema imposta pela capacidade de registo e controlo de acontecimentos relacionados com ações dos utilizadores, é necessário que o sistema integre condições que possibilitem a identificação dos mesmos possibilitando assim o relacionamento a

um conjunto distinto de procedimentos. Pretende-se que o processo de identificação possa ser efetuado o mais simplificadamente possível, traduzindo-se como vantagem na sua utilização. Estudado um conjunto de tecnologias que possibilitam a identificação de indivíduos, o autor reúne num comparativo as características vantajosas e desvantajosas de destaque de cada uma delas relativamente à sua integração no sistema (quadro 3.3).

Quadro 3.3: características das tecnologias de suporte à identificação (24) (39)(adaptado)

Tecnologia / Metodologia	Vantagem	Desvantagem
Código de Barras	Custos de utilização reduzidos	Fácil captura da informação
Código QR	Fácil utilização	Fácil captura da informação
Biometria	Alto nível de Segurança	Invasiva para o utilizador
Credenciais (Username e Password)	Processo de identificação e autenticação diferenciados	Processo desajustado para os pontos de acesso
RFID	Invisibilidade da informação	Recurso a objeto físico
NFC	Integração da funcionalidade portadora da informação no sistema do smartphone	Número atualmente reduzido de dispositivos que integram a tecnologia

Realizando um comparativo entre as tecnologias, as que apresentam características que possibilitam a fácil captura da informação são inadequadas ao sistema, uma vez que comprometeriam facilmente a segurança do mesmo. Relativamente aos processos biométricos, estes, apesar da segurança elevada que traduzem, poderiam ser interpretados como invasivos para o utilizador, podendo este rejeitar a sua utilização. O acesso através de credenciais, ainda que seguro, é desajustado tanto pelo necessário reconhecimento dos dados por parte do utilizador, como para o procedimento junto dos dispositivos de validação de acessos, tanto a espaços como a serviços.

No que respeita às duas restantes tecnologias não abordadas neste comparativo, ambas definem características que possibilitam a sua integração no sistema, contudo a implementação da tecnologia NFC num sistema cujos utilizadores, na sua maioria, poderão não assumir um acompanhamento tecnológico satisfatório, constituirá desajustes que colocará em causa a potencialidade do sistema atualmente. A tecnologia em questão, apesar da compatibilidade e ajuste com diversas funcionalidades, só agora começa a ser integrada num conjunto significativo de equipamentos disponíveis no mercado. A tecnologia RFID ainda que mais limitada, representa uma interação com o sistema simplificada para o utilizador, uma vez que recorre à utilização de equipamentos que não requerem ao utilizador qualquer interação tecnológica, são de fácil portabilidade e fisicamente admitem formatos de objetos comuns como, por exemplo, Cartões e pulseiras.

Reunidas as conclusões do comparativo, o autor, pelas características que melhor ajuste apresentam com o sistema, seleciona a tecnologia RFID como suporte aos processos de identificação dos utilizadores nos diversos locais de validação de acessos a espaços e serviços.

3.4 Sistemas de Identificação e Validação de Acessos

Embora a metodologia de identificação seja genérica para todo o sistema, os processos de validação de acesso a serviços e a espaços serão diferentes. O processo de validação de acesso a um espaço físico consiste em identificar o utilizador junto ao dispositivo do local e, de acordo com essa informação, retornar uma resposta referente à validação. Se a resposta for afirmativa um sinal elétrico deverá ser aplicado de forma a permitir a abertura da porta que lhe dará acesso, caso contrário a porta irá manter-se fechada. O processo de validação de acesso a um serviço consiste inicialmente, tal como o anterior, em identificar o consumidor, porém é posteriormente necessário selecionar o serviço ao qual pretende validar a permissão de acesso, ou seja, é necessária a introdução manual de informação adicional para que o processo possa decorrer corretamente. Retornada a resposta referente à validação, deverá ser efetuada a confirmação do acesso ao serviço através do respetivo registo, caso o utilizador o pretenda realizar. Uma vez que os processos são distintos, o sistema requer diferentes metodologias processuais para a realização de cada um deles.

3.4.1 Identificação e validação de acessos a serviços

Pela necessária introdução de informação adicional para além da referente à identificação do utilizador, a validação do acesso a um determinado serviço e a sua confirmação dependem de uma interface que possibilite o utilizador responsável pela prestação do respetivo serviço interagir com o sistema. Sendo genérico que qualquer entidade prestadora de serviços se encontre dotada de pelo menos um computador nas suas instalações para diversas funcionalidades, o autor apresenta uma solução que recorre a esse mesmo equipamento com o intuito de rentabilizar recursos, tornando o sistema mais eficiente. Recorrendo a este dispositivo será possível aceder a uma interface de interação com o sistema.

Uma vez que a identificação do utilizador, que pretende aceder ao serviço, será efetuada com recurso a etiquetas RFID será necessário garantir que ao mesmo computador se encontra conectado um dispositivo que possibilita a interação com estas, a fim de possibilitar este processo inicial.

Figura 3.3: sistema de validação de permissões de acesso a serviços (f.p)

O dispositivo interação com as etiquetas RFID deverá estabelecer comunicação com o computador através de uma interface de comunicação universal (USB) evitando a impossibilidade de ocorrência de incompatibilidades de conexão entre os dispositivos.

Efetuado o processo de identificação do consumidor e selecionada a informação adicional, o utilizador responsável pela prestação do serviço receberá o veredito da validação. Caso a resposta seja afirmativa, o utilizador responsável pela prestação deverá confirmar o acesso, registando no sistema se assim for a intenção do utilizador que efetuou a validação.

Reunidas as características processuais do sistema de validação de acessos a serviços, é requerido uma estrutura interativa semelhante à esquematizada pela figura 3.3.

3.4.2 Identificação e validação de acessos a espaços

Requerendo o processo de validação de acesso a um espaço somente a identificação do utilizador e do espaço, esta revela-se simplificada face à anterior. Resultando somente na atuação elétrica de um equipamento caso o acesso ao respetivo espaço seja permitido, todo o processo deverá decorrer sem a necessidade de um responsável por administrar a permissão, sendo este processo automatizado. Reunidas as características que definem o processo descrito, o autor apresenta três estruturas por ele concebidas e que cumprem as condições impostas.

Com base num computador como central de validação e comunicação com o servidor

A solução, demonstrada pela figura 3.4, propõe o recurso a um computador como equipamento responsável por processar a validação e registar no servidor a informação referente aos acessos.

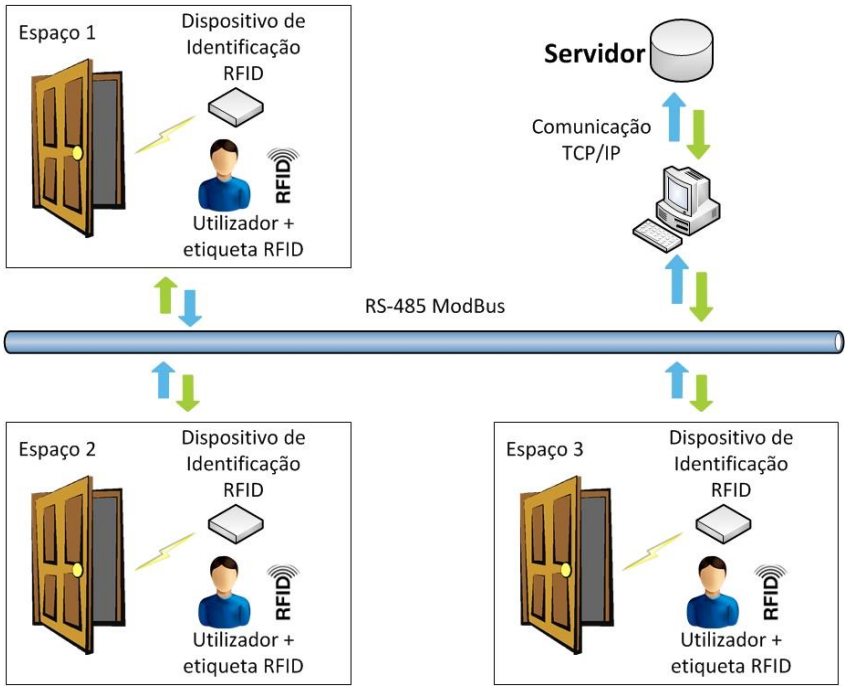


Figura 3.4: sistema baseado numa rede RS485 e com recurso a um computador (f.p)

A solução prevê que, por cada computador estejam associados um conjunto de dispositivos de identificação de forma a rentabilizar a sua utilização. A comunicação, entre os módulos de identificação e validação instalados junto às portas de acesso, é efetuada segundo o protocolo Modbus, cuja rede física de ligação é RS-485 (45). Apesar da solução apresentar uma estrutura robusta, o recurso a um computador poderá constituir uma desvantagem em instalações em que a sua utilização para funções paralelas seja dispensável. A infraestrutura de comunicação, também ela, poderá ser desajustada ao tipo de instalações previstas, dado que, em edifícios pré-construídos, seria necessária a instalação desta. Dada a dependência por uma rede de comunicação deste tipo, o sistema poderia tornar-se inadequado, perdendo o potencial que deve admitir.

Com base em módulos de validação e comunicação integrada com o servidor

Com o intuito de eliminar o recurso a um computador e uma infraestrutura de rede desajustada ao meio, o autor apresenta uma segunda solução, na qual, o recurso a um computador torna-se desnecessário. A solução propõe que cada um dos dispositivos de identificação estabeleça ligação diretamente com o servidor (figura 3.5). Para isto é imposto que estes dispositivos integrem a capacidade de estabelecer ligação através do protocolo TCP/IP (45).

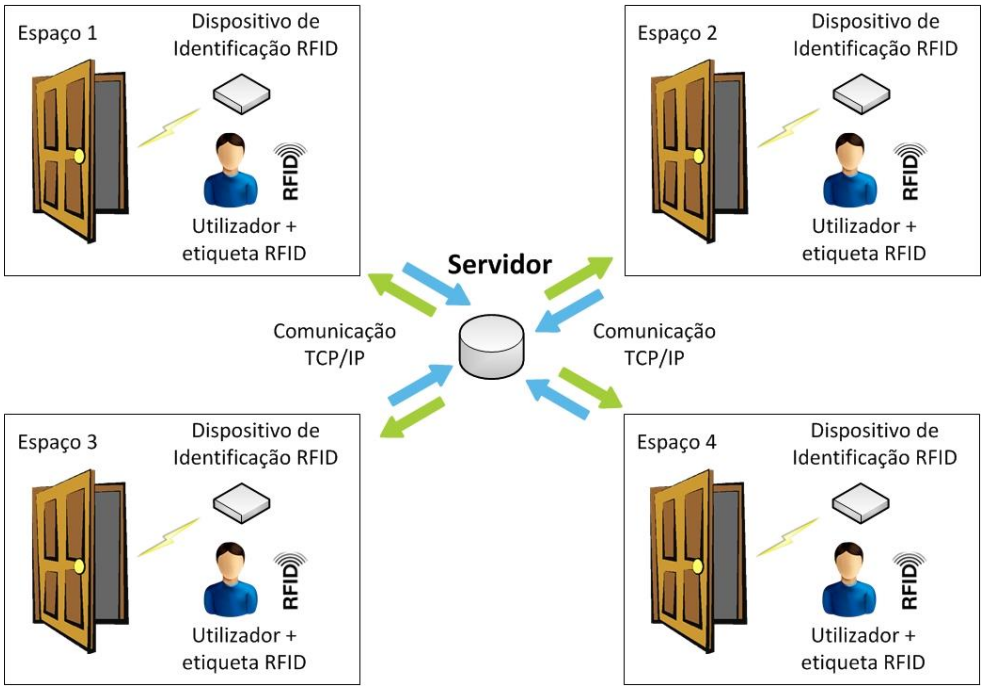


Figura 3.5: sistema baseado em dispositivos de comunicação direta com o servidor (f.p)

Embora a solução apresente remodelações que a potencializem face à anterior, como a exclusão de uma infraestrutura de comunicação desajustada do meio, impõe a cada um dos dispositivos de identificação uma maior capacidade de processamento e requisitos de interface com as redes de comunicação que suportem o protocolo TCP/IP (45), imposições estas que acrescem os custos de cada um dos dispositivos. Para além desta situação, a solução, caso admitisse somente ligação à rede por cabo, exigiria o acesso a cabos UTP junto a cada porta de acesso. Contrariamente, poderiam ser admitidas ligações Wi-Fi mas, mais uma vez, esta capacidade arrecadaria custos acrescidos para cada dispositivo, os quais em grande porção poderiam representar um orçamento de instalação do sistema exorbitante, tornando-se inadequado.

Com base num módulo central de comunicação com o servidor e com comunicação sem fios com os equipamentos de validação

Por fim, e de forma a contornar as desvantagens evidenciadas pelas soluções anteriormente descritas, o autor apresenta uma terceira solução para o sistema de identificação e validação de acessos a espaços. Esta solução, tal como a primeira, volta a impor um equipamento

central de comunicação com o servidor porém, nesta solução, este não corresponderá a um computador. Este módulo central será um dispositivo desenvolvido ajustadamente às funções que lhe serão requeridas.

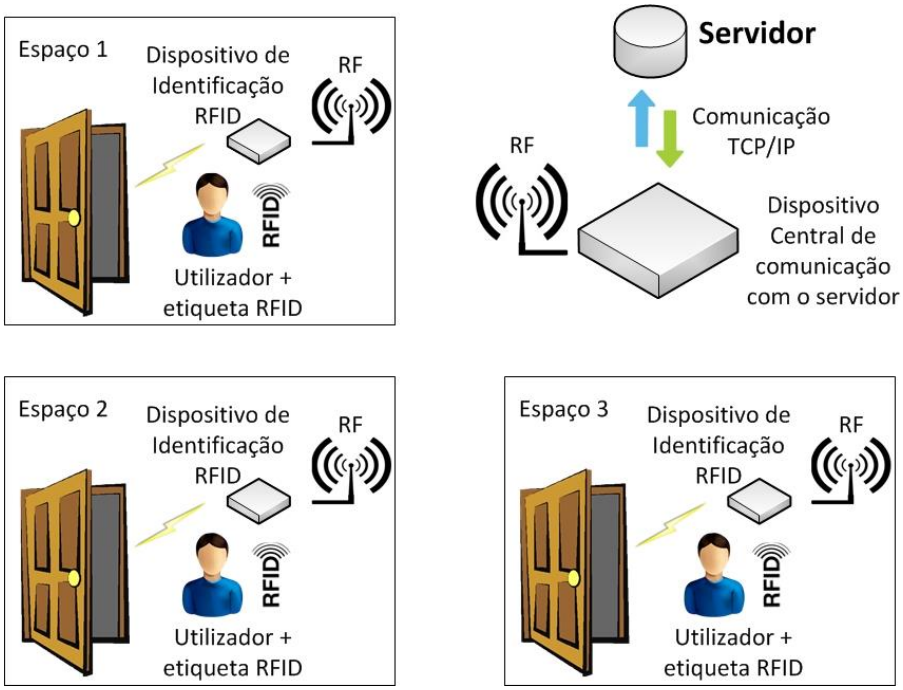


Figura 3.6: sistema baseado num dispositivo central de comunicação com o servidor (f.p)

Nesta solução, o autor propõe ao sistema a independência de redes de comunicação cabladas. Com base nesta abordagem, o autor recorre a tecnologias de comunicação sem fios para apresentar uma solução desprendida de requisitos que possam traduzir-se em desajustes de aplicação. Uma vez que as distâncias entre os dispositivos dispersos pelo interior de um edifício devem ser relativamente pequenas e as mensagens transmitidas entre eles não deverão integrar elevados níveis de informação, o autor propõe uma solução sem fios baseada na tecnologia de comunicação Zigbee. Com recurso a esta, para cada conjunto de dispositivos, poderá ser criada uma rede de comunicação, que possibilite a transmissão de dados entre os dispositivos de identificação e validação junto aos acessos e o módulo central, que comunicará com o servidor, possibilitando a recolha e inserção de dados nele. Nesta abordagem, a instalação do sistema requer somente o acesso a fontes de energia nos locais de instalação dos dispositivos (figura 3.6).

3.5 Software de Interface com o Sistema de Informação

O funcionamento integral do sistema depende, para além de todos os dispositivos e da arquitetura que os suporta, de uma ou várias interfaces computacionais que possibilitem a gestão de toda a informação do sistema. Uma vez que qualquer dispositivo conectado à rede Internet poderá estabelecer ligação com o servidor do sistema, é necessário garantir, por questões de segurança, que somente um determinado conjunto de dispositivos (os dispositivos constituintes do sistema) possam aceder à informação.

Sendo ainda evidente que a o acesso à informação não deverá ser acessível de modo generalizado a todos os utilizadores do sistema, é necessário definir estratégias que possibilitem o acesso personalizado à informação, estabelecendo assim um conjunto de características que definam um credível funcionamento do mesmo, principalmente no que refere a segurança da informação.

3.5.1 Interface do sistema de informação

Dado que o acesso ao sistema de informação será possibilitado somente a funcionários das diversas entidades associadas ao sistema e devidamente autorizados, o autor considera o sistema de informação do tipo *BackOffice*. Pela necessária interação com as etiquetas de identificação dos utilizadores, efetuada com recurso aos dispositivos periféricos a desenvolver, o autor considera ainda que o acesso ao sistema será efetuado com recurso a dispositivos robustos como computadores *Desktop* e *Laptop*. Baseado nestas condições, o autor apresenta duas plataformas de suporte a interfaces interativas a partir das quais pode ser desenvolvida a de acesso ao sistema de informação.

Página Web

- Acesso ao sistema possível através de um *webbrowser*;
- Interação com o sistema através de qualquer dispositivo que suporte um *webbrowser*;
- O acesso ao sistema é independente do sistema operacional do dispositivo;
- Utilização intuitiva;
- A interação com dispositivos ou funcionalidades locais aos dispositivos é dificultada sendo necessários *plugins* específicos que o possibilitem;
- Interface alojada no servidor;

Aplicativo

- O acesso ao sistema é possível somente através da aplicação;
- A aplicação pode ser incompatível com o sistema operativo do dispositivo, impossibilitando o acesso ao sistema através deste;
- Fácil interação com dispositivos localmente conectados;
- Interface alojada no dispositivo.

Realizando um comparativo entre as duas plataformas de suporte, o autor verifica que, apesar da dificultada garantia de compatibilidade com a generalidade dos dispositivos, o recurso a uma interface com base num **aplicativo** apresenta um conjunto de características que melhor ajuste definem com as condições funcionais esperadas para o sistema. A melhor capacidade de interação com dispositivos periféricos e a restrição de acesso ao sistema aos dispositivos que não a integrem são as características que o autor realça para a sua seleção.

3.5.2 Acesso personalizado ao sistema de informação

Embora selecionada uma plataforma que restringe o acesso a dispositivos que não integrem a interface, o acesso generalizado à informação a qualquer um deles representa ainda uma falha de segurança para o sistema, impossibilitando a credibilidade funcional do mesmo.

De modo a contornar esta situação, devem ser encontradas metodologias que, por um lado, permitam a definição do conjunto de informação à qual o utilizador da interface deverá ter acesso e, por outro, possibilitem associar os processos de edição de informação aos utilizadores responsáveis pela execução dos mesmos. Com esta segunda situação, a execução propositada de procedimentos danosos será teoricamente nula, dado que o responsável será identificado. No cumprimento destas condições, o sistema assumirá uma metodologia funcional que não só irá prever a segurança da informação, como também possibilitará assegurar a correta utilização do sistema.

Para possibilitar que o sistema responda corretamente às condições descritas, é necessário que um conjunto de informação possa ser interpretado e processado pelo mesmo. Sendo imposto que todos os processos devem estar associados ao utilizador responsável que interage com a interface, é necessário associar a este um conjunto de dados que possibilitem a sua identificação global no sistema. Por questões de segurança, o sistema deverá certificar a autenticidade do utilizador identificado.

Dado que o sistema já integra, através de etiquetas RFID, a capacidade de identificar os utilizadores nos processos de validação para acesso a serviços e a espaços, esta mesma metodologia de identificação poderia ser considerada para a identificação dos utilizadores no acesso à interface do sistema de informação, contudo e uma vez que a interação com a interface é prevista a utilizadores internos às entidades que integram o sistema, a dependência de objetos físicos para possibilitar o acesso a uma plataforma computacional pode ser desajustada. Baseado no processo integrado pela maioria das aplicações computacionais, que requerem identificação do utilizador, o autor seleciona a metodologia de identificação e autenticação que recorre a credenciais de acesso, ou seja, *Username* e *Password*. Através desta metodologia, o sistema admite a capacidade de determinação e reconhecimento dos utilizadores que acedem à interface do sistema de informação.

Contrariamente ao que sucede para os acessos aos serviços e espaços, os utilizadores não necessitam de objetos de identificação para acesso à interface, contudo devem conhecer as credenciais necessárias introduzir pelo que devem memoriza-las.

De acordo com cada utilizador reconhecido no acesso à interface, é possível configurar a informação detalhada à qual este poderá ter acesso, contudo, a seleção detalhada da informação a que é possível aceder, pode tornar-se um processo complexo pela diversidade de informação prevista pelo sistema. Por este motivo, o autor procura integrar estratégias que possibilitem definir tipos de utilizador, reduzindo a necessidade de seleção manual de detalhes comuns. Prevendo-se utilizadores que necessitam de acesso à informação global do sistema, utilizadores que necessitam de acesso a conjuntos limitados de informação e utilizadores que não devem aceder a qualquer informação, o autor sugere que a cada utilizador seja atribuído um estatuto, a partir do qual seja possível ao sistema criar automaticamente restrições de acesso à informação.

O autor, após reunir e estudar as atuais condições, verifica que o sistema revela ainda uma limitação na capacidade de estruturar corretamente o acesso à informação. Integrando cada entidade um conjunto de utilizadores de acesso à interface, é necessário que alguns destes consigam aceder para além da informação relacionada com os processos por si executados, a informação relacionada com os processos executados por outros utilizadores da mesma entidade. Esta situação prevê-se para utilizadores administrativos que devem aceder a todos os procedimentos relacionados com a entidade à qual pertencem. Embora seja necessário a estes utilizadores aceder a informações de processos de outros utilizadores, deve ser garantido que não acedem a informações de entidades alheias. O autor verifica que a associação de cada utilizador a uma entidade irá possibilitar que o sistema controladamente disponibilize a estes utilizadores

somente a informação a que devem aceder sem comprometer a credibilidade do sistema pelo acesso indevido a informações. Este processo depende da intersecção do parâmetro estatuto com o parâmetro entidade para cada utilizador.

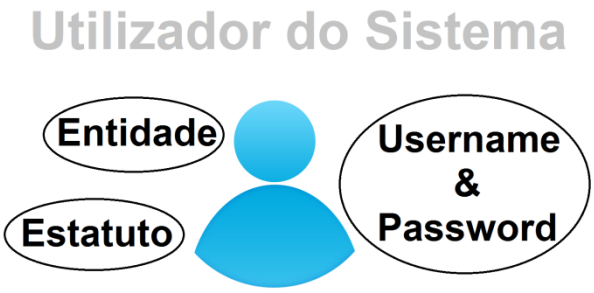


Figura 3.7: utilizador do sistema (f.p)

Respeitando a metodologia descrita, o autor verifica que se encontram reunidas as condições para que o sistema admita um funcionamento credível centrado no utilizador (figura 3.7), contudo, na sua implementação devem ser considerados no mínimo quatro estatutos de utilizador para que o sistema assim se comporte. O autor propõe e descreve a principal característica de perfil de cada um deles:

1. **Super Administrador:** poderá aceder a toda a informação do sistema.
2. **Administrador:** poderá aceder a informação de utilizadores da sua entidade
3. **Colaborador:** só poderá aceder a informação de processos efetuados por ele
4. **Cliente:** não poderá aceder à interface, não podendo aceder a qualquer informação

Capítulo 4 Implementação da Solução Proposta

Após a definição da arquitetura e metodologia funcional do sistema é necessário conceber e implementar os dispositivos constituintes necessários, bem como desenvolver as aplicações de interface que possibilitam a sua utilização. A figura 4.1 demonstra um cenário global para o sistema.

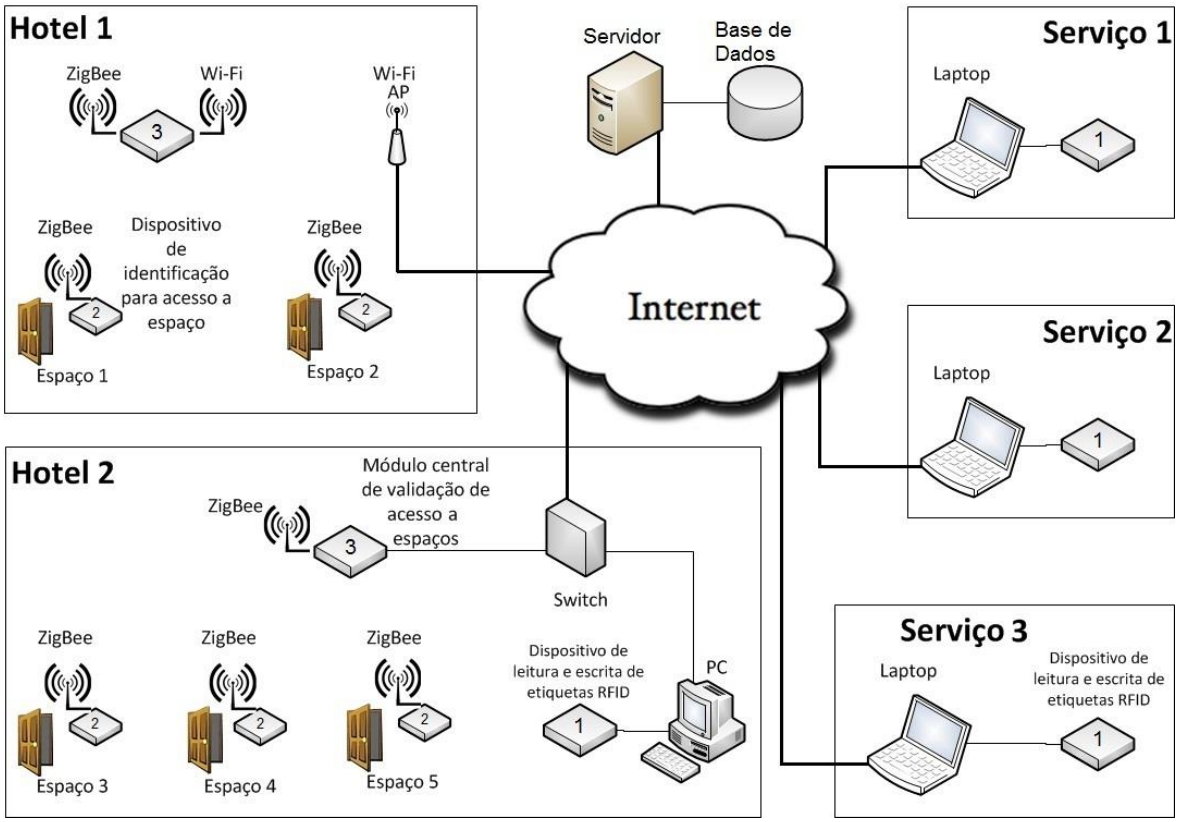


Figura 4.1: cenário Funcional do sistema (fonte própria)

Dado que o sistema integra dispositivos com diferentes funcionalidades, o processo descritivo de implementação será sequencial, individualizando cada um dos constituintes e relevantes no âmbito do trabalho desenvolvido. O mesmo cenário descritivo será efetuado para as aplicações de interface.

4.1 Dispositivos

O sistema integra um conjunto diverso de dispositivos, mas apenas prevê a conceção de três: dispositivos de leitura e escrita de etiquetas RFID e os dois dispositivos constituintes do sistema de validação de acessos a espaços. A abordagem aos restantes dispositivos necessários ao esperado funcionamento do sistema não será descriminada, uma vez que estes correspondem a dispositivos de acesso comercial e cujas características possibilitam a execução das funções impostas pelo sistema. Por este motivo, não é objetivo deste trabalho a conceção ou restruturação de dispositivos para além dos acima mencionados.

4.1.1 Equipamento de interação com etiquetas RFID

Uma vez que a identificação dos utilizadores será efetuada com recurso à tecnologia RFID, é necessário definir e conceber os dispositivos de interação com as etiquetas. Estes dispositivos serão constituídos por diversos equipamentos, sendo um deles o equipamento que possibilitará a interação com as etiquetas RFID.

4.1.1.1 Seleção do equipamento

De modo a selecionar um equipamento ajustado com as necessidades, o autor apresenta seguidamente dois atualmente acessíveis no mercado.

Equipamento Sparkfun

A entidade *Sparkfun* apresenta uma solução composta pelo módulo RFID Evaluation Shield-13.56MHz (46) e o módulo RFID Module-SM130 Mifare (13.56 MHz) (47). O primeiro refere uma PCB que integra a antena necessária para transmissão RF. O segundo refere o *modem* responsável por converter comandos em mensagens RF e vice-versa. A figura 4.2 demonstra os dois módulos constituintes.

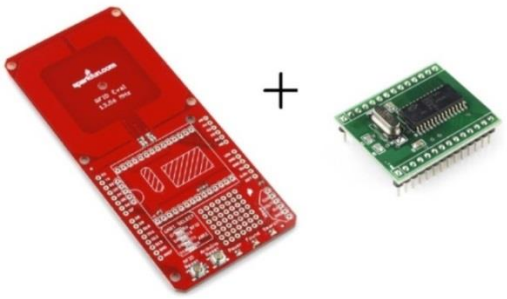


Figura 4.2: equipamento de Interação com etiquetas RFID Mifare (46)(adaptada)

Este equipamento é compatível com etiquetas RFID passivas do tipo Mifare (ISO/IEC 14443-A). A comunicação deste equipamento com o responsável por controlar o seu funcionamento (microcontrolador), pode ser estabelecida por I2C ou uma comunicação serie RS-232 níveis TTL.

Equipamento Adafruit

O segundo equipamento sugerido é o módulo PN532 NFC/RFID controller shield (48) da Adafruit (figura 4.3).

Figura 4.3: equipamento de Interação com etiquetas RFID e NFC (48)(adaptada)

Este equipamento demonstra compatibilidade com diversificadas etiquetas passivas RFID, bem como possibilita comunicação NFC. Relativamente a RFID, este equipamento é compatível com os seguintes protocolos:

- Mifare (ISO/IEC14443-A)
- Felica (212 kbps e 424 kbps)
- ISO/IEC14443-B
- Innovision Jewel tag

A comunicação entre este equipamento e o responsável pelo controlo funcional (microcontrolador) é estabelecida por I2C ou por SPI.

Comparando os dois equipamentos, o autor verifica, que ambos apresentam custos de aquisição próximos, no entanto o equipamento da Adafruit pela maior abrangência apresenta-se vantajoso face ao equipamento da Sparkfun. Uma vez previsto o recurso a microcontroladores como responsáveis pelo controlo funcional, qualquer das comunicações admitidas por estes equipamentos podem ser estabelecidas com os microcontroladores. Reunidas e comparadas as características, o autor seleciona o equipamento **PN532 NFC/RFID controller shield** da Adafruit como equipamento que irá ser integrado nos dispositivos que assim o requeiram na sua constituição.

4.1.1.2 Adaptação e funcionamento

De modo a reduzir falhas de funcionamento e dificuldades de perceção do mesmo, o equipamento de interação com etiquetas RFID foi embutido numa estrutura albergadora juntamente com três sinalizadores luminosos (*leds*), tal como demonstra a figura 4.4. Por questões descritivas, o autor denominou este conjunto como módulo de interação com etiquetas RFID.

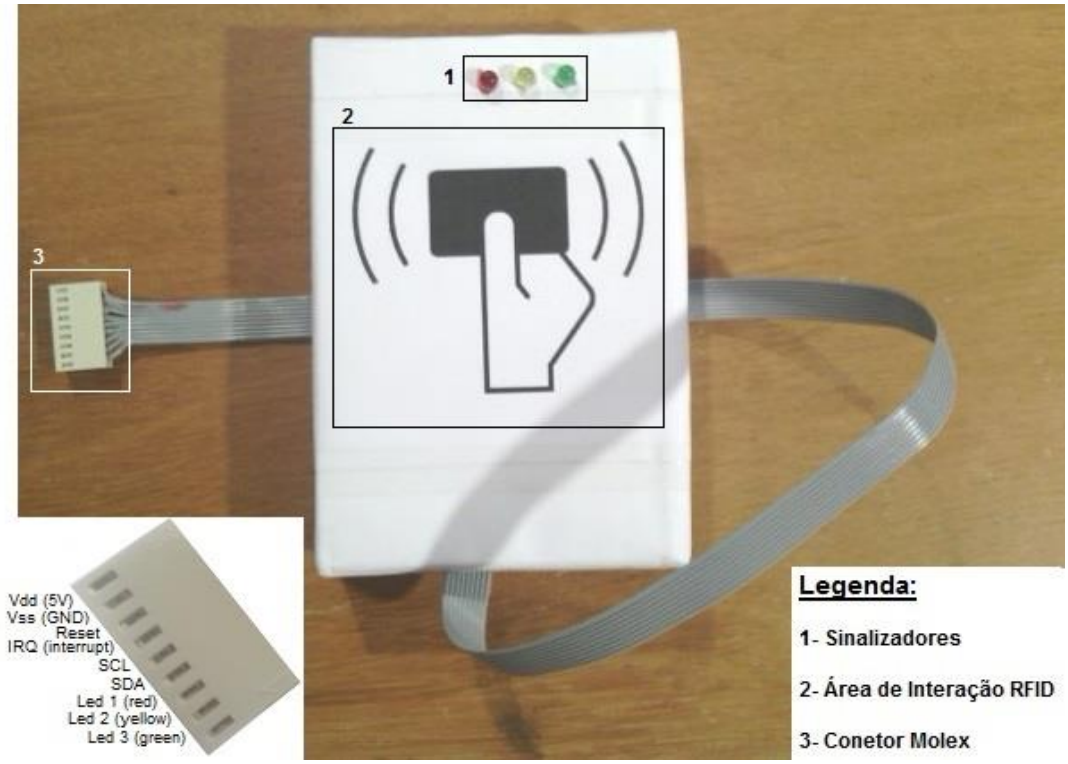


Figura 4.4: módulo de interação com etiquetas RFID (f.p)

A ligação aos *leds* e ao equipamento é efetuada através do conector Molex cuja descrição é efetuada na figura 4.4. Como é possível verificar, neste conector não se encontram disponíveis ligações à interface de comunicação *SPI* do equipamento de interação com as etiquetas RFID. Esta situação deve-se ao facto do autor do trabalho ter selecionado a interface de comunicação I2C como a que será utilizada. Esta seleção não admitiu qualquer outro critério para além do facto de esta interface ser a, por defeito, definida pelo fabricante do equipamento. É possível verificar que através do conector é possível aceder à ligação a um pin de *Reset* e a um outro definido como IRQ. Através do pin *Reset* será possível reiniciar o dispositivo sem que para isso seja necessário desconectá-lo da alimentação. O acesso ao pin IRQ possibilitará sincronizar o microcontrolador com o equipamento de interação com etiquetas RFID durante alguns procedimentos funcionais, sendo a funcionalidade seguidamente explicada.

A necessária interação do equipamento com etiquetas RFID passivas depende de um conjunto de processos executados com recurso a um equipamento controlador. Este equipamento deverá controlar o equipamento de interação com recurso aos seguintes comandos:

- InListPassiveTarget (49) – Possibilita a deteção e o estabelecimento de comunicação com as etiquetas RFID, retornando dados necessários aos seguintes procedimentos.
- InDataExchange (49)– Possibilita efetuar autenticação, leitura/escrita num bloco da memória da etiqueta.

As mensagens referentes aos comandos são enviadas por I2C, uma vez que a interface SPI não se encontra ativa, sendo retornadas mensagens pelo equipamento de interação. O anexo 1 deste documento representa esquematicamente a interação por I2C. O equipamento de interação admite duas metodologias de comunicação, possibilitando com uma delas a redução de mensagens de sincronismo. Essa metodologia exige uma conexão física extra entre o controlador e o equipamento de interação, através do Pin IRQ do mesmo, responsável por indicar, pela variação dos níveis de tensão, ao controlador os momentos em que o equipamento de interação reúne informações e se encontra apto para o envio da mesma. No anexo 2 deste relatório encontram-se representados dois diagramas referentes à interação entre os equipamentos nas duas metodologias de comunicação referidas.

4.1.2 Etiquetas RFID

Uma vez que o equipamento de interação apresenta compatibilidade com diversos protocolos de comunicação *RFID* poderia ser adotada para o sistema qualquer etiqueta que respeitasse os protocolos suportados por este equipamento, contudo, o autor preferiu definir um só tipo de etiquetas com o intuito de reduzir probabilidades de erro por incompatibilidade. Sem recurso a qualquer outro critério para além dos custos de aquisição, o autor define etiquetas **Mifare (ISO/IEC 14443-A*)*** como as admitidas para o sistema. Embora possam surgir em diversos formatos físicos, considera-se que estas serão tipo cartão (figura 4.5).

Figura 4.5: exemplo de etiquetas RFID Mifare (tipo Cartão) (48)(adaptada)

A arquitetura da memória de dados das etiquetas *Mifare* encontra-se esquematicamente representada no anexo 3 deste documento.

4.1.3 Dispositivo de leitura e escrita de etiquetas RFID

O dispositivo de escrita e leitura corresponde ao periférico que possibilita a interação controlada pelo computador com as etiquetas RFID, como esquematiza a figura 4.6.

Figura 4.6: cenário de utilização do dispositivo (f.p)

Este dispositivo possibilitará recolher e inserir informação nas etiquetas de acordo com as necessidades dos processos executados pelas aplicações responsáveis por tarefas de registar

cartões, atribuir permissões de acesso a espaços e a serviços e validar acessos a serviços. Tal como a figura 4.7 demonstra, o dispositivo concebido pelo autor é constituído por um conversor USB 2.0 to serial (MCP2200) (50), por um microcontrolador (PIC18F2520) (51) e um módulo de interação com etiquetas RFID. O esquema elétrico do circuito desenvolvido encontra-se disponível no anexo 4.

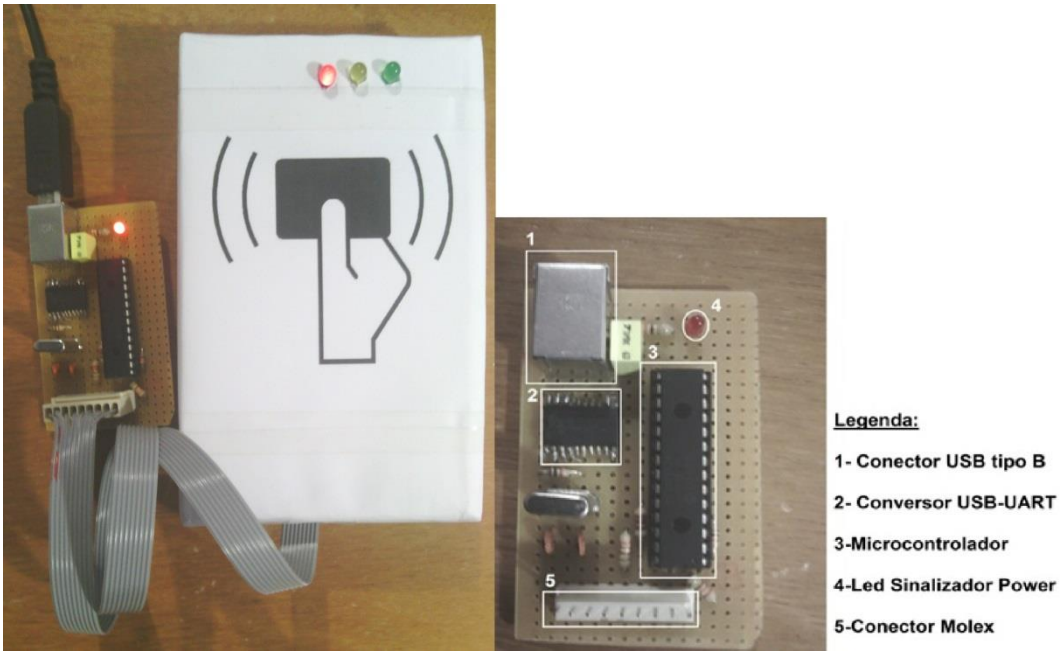


Figura 4.7: dispositivo de leitura e escrita de etiquetas RFID (f.p)

A conexão do dispositivo ao computador é efetuada fisicamente através de uma ligação USB sendo a comunicação estabelecida do tipo serie RS-232 (45) com os seguintes parâmetros de comunicação:

- BaudRate: 9600 bit/s
- Dados: 8 bit
- Paridade: Não
- Stop Bits: 1 bit
- Controlo de Fluxo: Nenhum

A conexão ao módulo de interação com etiquetas RFID é efetuada através do conector Molex (9 Pins) compatível com o conector que este integra.

A comunicação estabelecida entre o computador e o dispositivo permite a troca de mensagens entre eles, contudo o dispositivo só enviará uma mensagem caso o computador tenha

efetuado previamente uma requisição ao mesmo. As mensagens trocadas entre eles assumem estruturas definidas pelo autor do trabalho, as quais foram concebidas com base na estrutura das mensagens definidas pelo protocolo Modbus. As mensagens podem assumir duas funções distintas, ou seja, leitura e escrita, sendo desnecessário o endereçamento tanto do destinatário como do remetente, uma vez que a comunicação é estabelecida sempre entre dois dispositivos. Na estrutura definida, o campo função é formado por um byte, podendo este assumir os valores caracter 3 e caracter 6, correspondendo respetivamente a leitura e a escrita. Caso a mensagem emitida seja do tipo leitura, o campo mensagem é inexistente, sendo o tamanho da mensagem igual a cinco bytes. A figura 4.8 esquematiza a estrutura das mensagens enviadas pelo computador.

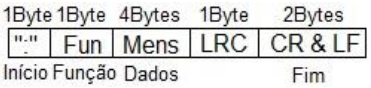


Figura 4.8: estrutura das mensagens enviadas do computador para o dispositivo (f.p)

Após o envio de uma mensagem pelo computador, o dispositivo irá emitir uma de retorno até um tempo máximo de cinco segundos após o envio da mensagem de requisição. Caso o dispositivo não retorne qualquer mensagem após este tempo, a aplicação responsável pelo envio deverá assumir que a mensagem não foi corretamente recebida pelo dispositivo. A figura 4.9 apresenta esquematicamente a estrutura das mensagens enviadas pelo dispositivo.

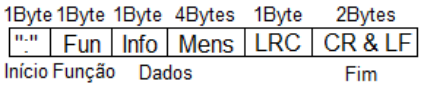


Figura 4.9: estrutura das mensagens de resposta do dispositivo (f.p)

Quando o dispositivo retorna uma mensagem para o computador, o campo função é preenchido com o mesmo valor do da mensagem de requisição e, contrariamente às mensagens emitidas pelo computador, quando a função é do tipo leitura, a mensagem enviada pelo dispositivo incorpora o campo mensagem. Esta mesma mensagem incorpora ainda o campo Info, através do qual é possível retornar para a aplicação informação referente à interação efetuada pelo dispositivo com a etiqueta RFID. Este campo admite três valores distintos, ou seja, carater 0, carater 1 e carater 2, os quais, correspondem respetivamente, sucesso na interação, erro na interação com a etiqueta e etiqueta não encontrada dentro do tempo máximo estabelecido. O

diagrama representado na figura 4.10 demonstra dois exemplos de interação. O primeiro exemplifica a leitura de 16 bytes de dados de um cartão e o segundo a escrita de um novo valor. Ambos são bem-sucedidos uma vez que o campo informação é preenchido com o valor 0 pelo dispositivo.

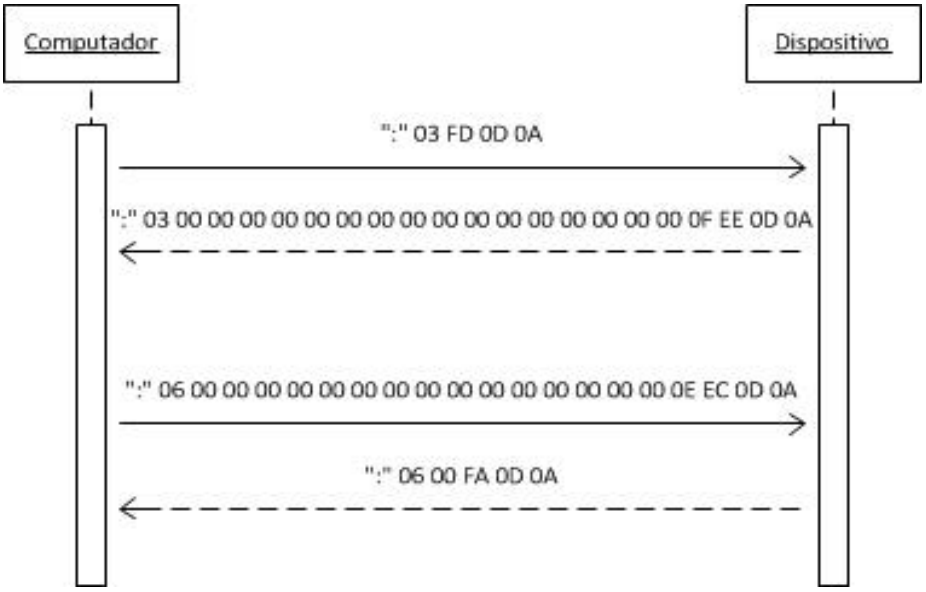


Figura 4.10: diagrama de comunicação entre o computador e o dispositivo (f.p)

Embora o módulo de interação com etiquetas seja comum a diversos dispositivos, os *leds* de sinalização constituintes poderão admitir comportamentos distintos para cada um deles. Para o caso do dispositivo em questão, o *led* vermelho sinaliza a conexão do dispositivo, ou seja, este *led* indica se o dispositivo se encontra pronto para utilização. O *led* verde sinaliza a procura por etiqueta, ou seja, este *led* acenderá quando for emitida uma ordem pelo computador para interagir com uma etiqueta, mantendo-se ligado por um período máximo de cinco segundos. A interação só será possível enquanto este *led* se mantiver ligado. Por fim, o *led* amarelo é o sinalizador de erros, podendo este assumir dois distintos comportamentos. A intermitência deste *led* será visível quando uma ordem de interação for enviada e nenhuma etiqueta for encontrada pelo equipamento após cinco segundos (*time out*) do envio da ordem de interação. A presença continua deste *led* indica que, após ordem de interação, uma etiqueta foi encontrada, porém ocorreu um erro que impossibilitou o sucesso do procedimento em curso.

4.1.4 Dispositivos constituintes do sistema de validação de acessos a espaços

O sistema de validação de acessos a espaços é constituído por dois dispositivos distintos, ou seja, dispositivo de identificação para acesso a espaços e módulo central de validação de acesso a espaços (figura 4.11).

Figura 4.11: cenário funcional dos dispositivos do sistema (f.p)

Cada local de acesso, controlado pelo sistema, requer a instalação de um dispositivo de identificação para acesso a espaço junto à porta referente. Através deste dispositivo será efetuada a identificação por RFID, o qual deverá enviar toda a informação (identificação da etiqueta e identificação do local) para o módulo central de validação de acessos a espaços. Este irá validar o acesso contactando o servidor e retornará o veredito para o dispositivo de identificação para acesso a espaços, o qual atuará de acordo com essa informação.

Cada módulo central poderá ter associado um vasto conjunto de dispositivos de identificação não sendo necessário um módulo por cada um destes dispositivos. Dado o princípio de funcionamento, é implícito que os diversos dispositivos comuniquem entre si e dada a dispersão destes pelas instalações hoteleiras, o autor estruturou o sistema recorrendo a tecnologias de comunicação sem fios, simplificando os requisitos para instalação e funcionamento do sistema.

Tendo o autor do trabalho recorrido à tecnologia de comunicação sem fios Zigbee, como método de possibilitar a comunicação entre dispositivos, a quantidade de dispositivos de

identificação associados por cada módulo central será definida pelas distâncias entre eles. Esta situação deve-se ao facto da distância máxima de comunicação entre os dispositivos ser limitada a 100m, em campo aberto. A tecnologia impõe ainda um limite de dispositivos por rede (65536 teoricamente), contudo este dificilmente será atingido pelo sistema num cenário real. Não podendo ser definido um valor exato de dispositivos de identificação associados por módulo, a quantidade irá variar de acordo com a estrutura das instalações onde o sistema seja aplicado.

4.1.4.1 Equipamento de comunicação Zigbee

De entre diversos dispositivos de comunicação compatíveis com a tecnologia Zigbee, o autor destaca os dois que melhor se ajustam às características dos dispositivos integradores.

Módulo XBee da DIGI (52)

Figura 4.12: Módulos XBee (52)

Os módulos XBee (figura 4.12) integram um conjunto de interfaces digitais e analógicas, sendo a comunicação com o dispositivo estabelecida por uma ligação serie (45) (RS-232 níveis TTL) através da sua interface UART. Através desta é possível adquirir e alterar o estado das interfaces digitais e analógicas. Quando integrado numa rede Zigbee, este dispositivo permite a transmissão de dados entre dispositivos em modo transparente (transmissão de mensagens pelas interfaces UART) e ainda controlar e monitorizar interfaces de outros módulos remotamente. O controlo e monitorização das interfaces, tanto remotamente como localmente são efetuados com recurso a comandos AT.

Módulo Zigbee Uext da OLIMEX (53)

Figura 4.13: MOD-ZIGBEE-UEXT (53)

Os módulos Zigbee da Olimex (figura 4.13), contrariamente aos anteriores, não integram quaisquer funcionalidades pré-definidas, sendo o funcionamento deste totalmente configurável. A configuração é possível, uma vez que o equipamento disponibiliza o acesso à interface de programação do microcontrolador (PIC18F26k20) (54) constituinte, através de um conector mini ICSP. Integrando o equipamento um *transceiver* RF (MRF24J40) (55), cujas características de modulação são compatíveis com as previstas pela tecnologia de comunicação Zigbee, é possível configurá-lo de forma a integrá-lo como módulo desta tecnologia. A interface com o equipamento é efetuada fisicamente através de um conector UEXT no qual estão acessíveis seis terminais do microcontrolador (VDD-3.3V, GND, UART TX e RX e I2C SDA e SCL). O equipamento integra ainda dois leds e dois botões devidamente conectados a interfaces do microcontrolador.

Apesar do módulo XBee da Digi apresentar um funcionamento pré-definido, a possibilidade de configuração pormenorizada do funcionamento atribui ao módulo da Olimex características vantajosas no que refere a capacidade de adaptação com os equipamentos do dispositivo que o integrará. Embora esta característica represente uma vantagem nesta avaliação, também representa uma desvantagem dado que o funcionamento destes equipamentos depende de um processo de programação, o qual, para o equipamento XBee, não é necessário. Relativamente a custos de aquisição, os módulos da Olimex apresentam o preço inferior, definindo novamente uma vantagem a seu favor.

Baseado no comparativo descrito, o autor selecionou os **MOD-Zigbee-UEXT** da Olimex como o equipamento constituinte dos dispositivos do sistema de validação de acessos a espaços e responsável por possibilitar a comunicação entre eles. Relativamente à programação destes equipamentos, o autor destaca o esforço adicional requerido. Este processo foi realizado com recurso à *stack* Zigbee (56), disponibilizada pelo fabricante. O processo consistiu na restruturação dos programas de forma a ajustar o funcionamento dos equipamentos às características do

sistema. Deste processo resultam duas configurações distintas para os equipamentos, ou seja, coordenadores e dispositivos terminais. Após todo o rigoroso processo de restruturação e adaptação funcional dos equipamentos, é possível com recurso a estes, estabelecer uma rede de comunicação Zigbee com topologia estrela.

A estrutura das mensagens, tal como para o dispositivo de leitura e escrita de etiquetas RFID, foi concebida pelo autor com base na estrutura das mensagens do protocolo Modbus. Dependendo da configuração funcional dos equipamentos, estes irão enviar mensagens recebidas pela interface UART caso estas respeitem a estrutura definida para cada um deles. Numa abordagem genérica, as mensagens devem ser iniciadas com o caracter ":", conter um campo de validação (LRC) e finalizarem com os caracteres 13 e 10 nesta sequência. Especificamente a cada tipo funcional, o tamanho deve assumir um valor específico, sendo que equipamentos configurados como coordenadores admitem mensagens com tamanho total igual a 11 bytes, enquanto o tamanho admissível por equipamentos configurados como dispositivos terminais é de 26 bytes. O envio das mensagens, para além do cumprimento das especificações descritas, depende da validação do valor LRC que possibilitará identificar erros na mensagem. Na não deteção de qualquer erro, a mensagem será enviada. Após ser recebida pelo módulo recetor, a mensagem será novamente avaliada relativamente a erros, sendo remetida para a interface UART do módulo caso nenhum tenha sido verificado.

O estabelecimento da comunicação com estes equipamentos depende da correta definição dos parâmetros de comunicação serie no equipamento a conectar. Os parâmetros pré-definidos para a comunicação serie dos módulos são os seguintes:

- BaudRate: 19200 bits/s
- Dados: 8 bits
- Paridade: Não
- Stop Bits: 1 bit
- Controlo de Fluxo: Nenhum

As mensagens enviadas pelos equipamentos configurados como dispositivos terminais são sempre entregues ao equipamento configurado como coordenador. Por sua vez, este equipamento só possibilita o envio de mensagens para equipamentos configurados como dispositivos terminais caso tenha recebido alguma por parte destes.

As mensagens trocadas entre dispositivos são semelhantes quando comparadas antes e depois do envio, contudo durante o processo de transmissão sem fios esta semelhança não se verifica. As mensagens, previamente ao envio por RF são restruturadas, sendo novamente convertidas para o estado original logo após a receção pelo equipamento respetivo. Este processo deve-se à necessidade de transmissão de dados referentes à comunicação RF entre os equipamentos. A junção destes dados com os da mensagem original numa única e nova mensagem deve-se à necessidade de garantir que nunca ocorre a falha de receção parcial de dados. Os dados extra enviados serão utilizados para que o equipamento coordenador possa definir e gerir uma tabela de redireccionamentos. Com recurso a esta tabela é possível garantir o envio de mensagens de resposta somente para os equipamentos configurados como dispositivos terminais que previamente enviaram mensagens. Com a utilização desta metodologia, é possível garantir condições de segurança necessárias ao funcionamento fiável do sistema.

O comportamento funcional dos equipamentos foi especificamente configurado para que estes apresentem o melhor ajuste com as necessidades dos dispositivos que os integram. Toda a configuração funcional foi programada pelo autor do trabalho, o qual, para além desta, adaptou o funcionamento dos equipamentos a outros possíveis cenários. A descrição pormenorizada da programação dos equipamentos para outras funcionalidades encontra-se disponível no anexo 7 deste documento.

4.1.4.2 Dispositivo de identificação para acesso a espaço

Este dispositivo prevê a sua instalação junto às portas de acesso aos espaços, sendo responsável por possibilitar a identificação por RFID e pela atuação elétrica da fechadura da respetiva porta, caso seja verificada permissão de acesso ao utilizador (figura 4.14).

Figura 4.14: cenário funcional do dispositivo (f.p)

Este equipamento é constituído por um microcontrolador (PIC18F2520) (51), por um relé que possibilitará fechar o circuito de alimentação da fechadura, por um acoplador UEXT responsável por possibilitar a conexão do equipamento de comunicação que efetuará a transmissão de dados com o módulo central de validação de acessos a espaços (módulo Zigbee) e por um módulo de interação com as etiquetas RFID (figura 4.15). Este dispositivo requer ainda alimentação através de uma fonte externa 9V DC 100mA. O esquema elétrico do circuito desenvolvido encontra-se disponível no anexo 5.

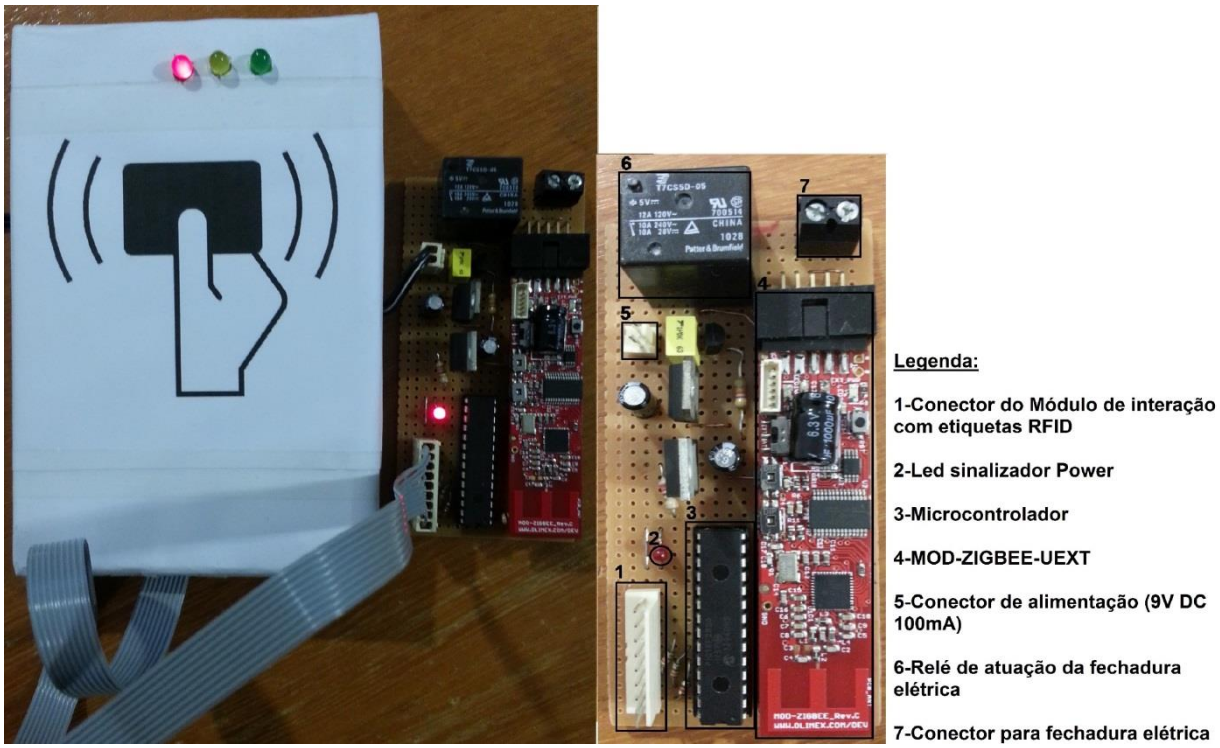


Figura 4.15: dispositivo de identificação para acesso a espaço (f.p)

O dispositivo encontra-se endereçado com um código de identificação do local (quatro bytes, único no sistema e registado no microcontrolador). Na ocorrência de tentativa de acesso por parte de um utilizador, o microcontrolador irá recolher a informação da etiqueta (código de 16 bytes) e, juntamente com o código de identificação do local, irá compor a mensagem que deverá enviar para o equipamento de comunicação Zigbee, configurado como dispositivo terminal, o qual a enviará por RF para o módulo central de validação. A mensagem enviada pelo microcontrolador para o equipamento Zigbee admite a estrutura concebida pelo autor, tendo sido esta definida com base na estrutura das mensagens Modbus.

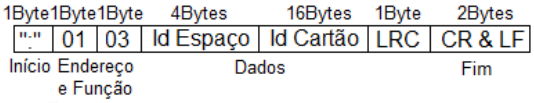


Figura 4.16: estrutura da mensagem de validação enviada pelo dispositivo (f.p)

Como é possível observar pela estrutura representada na figura 4.16, os campos endereço e função apresentam valores definidos. Esta situação deve-se ao facto destes campos não serem necessários ao atual funcionamento do sistema. O campo endereço é desnecessário uma vez que as mensagens originadas nestes dispositivos terão sempre como destino o módulo central de validação de acesso a espaços. De igual modo, o campo função também não é necessário dado que somente um procedimento será possível, ou seja, validação do acesso. Apesar desta situação, o autor preferiu integrar estes campos na estrutura da mensagem por questões de coerência, isto é, mantendo os campos enunciados, a mensagem apresenta uma maior relação de semelhança com a estrutura de mensagem utilizada como referência, bem como, lhe define a capacidade de agregar mais dois bytes de informação em necessidades futuras, sem que para isso sejam requeridas alterações de grande impacto.

Após envio da mensagem para o módulo central de validação, este deverá efetuar o processo pelo qual é responsável, retornando uma resposta para o dispositivo de identificação. Caso não seja retornada qualquer mensagem de resposta após um segundo do envio da mensagem inicial, o dispositivo irá considerar que o módulo central de validação não se encontra em condições funcionais. Esta situação poderá ser facilmente percebida, dado que o *led* sinalizador amarelo, do módulo de interação com as etiquetas RFID constituinte, irá demonstrar um comportamento intermitente acelerado durante um segundo. Caso esta situação não se verifique e uma mensagem seja retornada, o microcontrolador irá processar a informação recebida. A figura 4.17 representa a estrutura da mensagem de resposta enviada pelo módulo central de validação. Tal como as anteriores estruturas de mensagem concebidas pelo autor, também esta assume por referência a estrutura das mensagens Modbus.

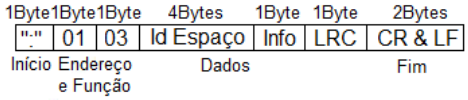


Figura 4.17: estrutura da mensagem de resposta à validação do acesso (f.p)

Embora o retorno da mensagem seja garantidamente efetuado para o dispositivo de identificação que iniciou o processo de validação, por questões de segurança, o microcontrolador

do dispositivo de identificação para acesso a espaços deverá comparar o seu código de identificação do espaço com o da mensagem de resposta, eliminando qualquer possibilidade de abertura de uma porta erradamente, situação que poderia ser provocada por um incorreto reencaminhamento de mensagem de retorno. Caso verifique igualdade, irá processar a informação referente à validação contida no campo Info. Este campo pode assumir quatro valores distintos:

- Caracter 0: registo de validação efetuado com sucesso no sistema e acesso negado por inexistência atual de permissão para o utilizador. O *led* sinalizador vermelho do módulo de interação com as etiquetas deverá assumir um comportamento intermitente durante dois segundos.
- Caracter 1: registo de validação efetuado com sucesso e acesso permitido ao utilizador. O *led* verde acenderá continuamente durante dois segundos e o relé integrado pelo dispositivo irá atuar durante 100ms no decorrer desse intervalo, possibilitando a abertura da porta.
- Caracter 2: registo de validação sem sucesso. Falha de ligação com o servidor. O *led* sinalizador amarelo irá admitir um comportamento intermitente lento durante dois segundos.
- Caracter 3: registo de validação sem sucesso. Ligação estabelecida com o servidor, contudo ocorreu uma falha num dos processos intermédios. A sinalização é semelhante à anterior situação enunciada.

Quando o dispositivo se encontrar alimentado, o *led* sinalizador vermelho deverá estar ligado, indicando que o dispositivo se encontra em estado funcional e pronto a interagir com as etiquetas de identificação, possibilitando a validação de acessos. A figura 4.18 apresenta um diagrama de comunicação do dispositivo.

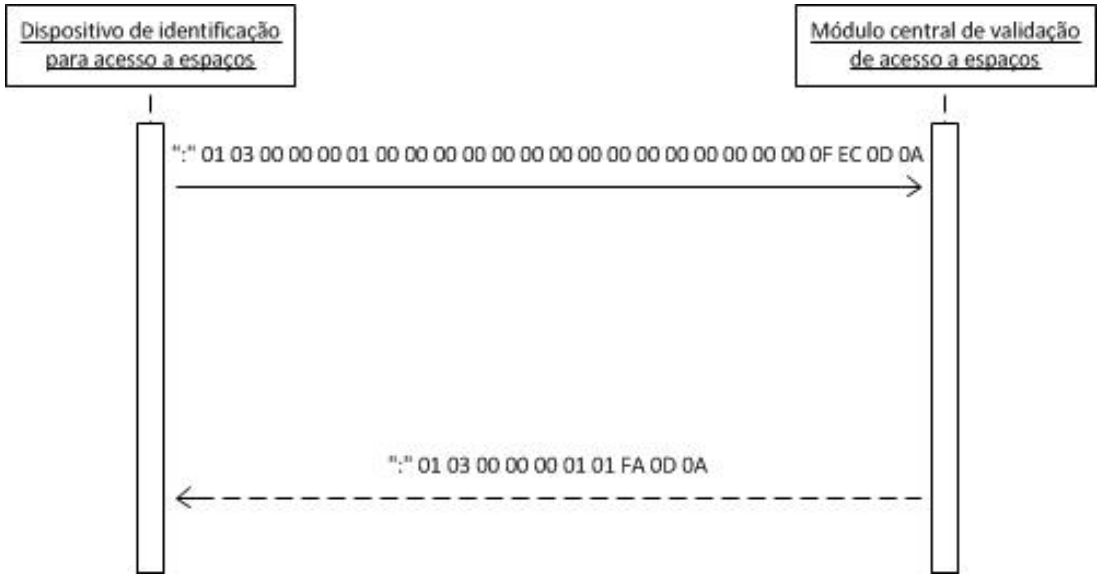


Figura 4.18: diagrama de comunicação do dispositivo (f.p)

4.1.4.3 Módulo central de validação de acesso a espaços

Este dispositivo é responsável por processar todos os pedidos de validação de acesso a espaços enviados por dispositivos de identificação a ele associados, retornando para estes o veredito após a validação (figura 4.19).

Figura 4.19: cenário funcional do dispositivo (f.p)

Este dispositivo é constituído por um microcontrolador (PIC32MX110F016B) (57), um conversor RS-232 to TCP/IP (Ethernet e Wi-Fi) (58), responsável por permitir a comunicação com a rede Internet, por dois *leds* sinalizadores e por um acoplador UEXT, responsável por possibilitar a conexão do equipamento de comunicação (módulo Zigbee) (53) que possibilitará a troca de informação com os dispositivos de identificação para acesso a espaços a si associados (figura 4.20). Este dispositivo, tal como o dispositivo de identificação para acesso a espaços, requer alimentação através de uma fonte externa 9V DC 150mA. O esquema elétrico do circuito desenvolvido encontra-se no anexo 6.

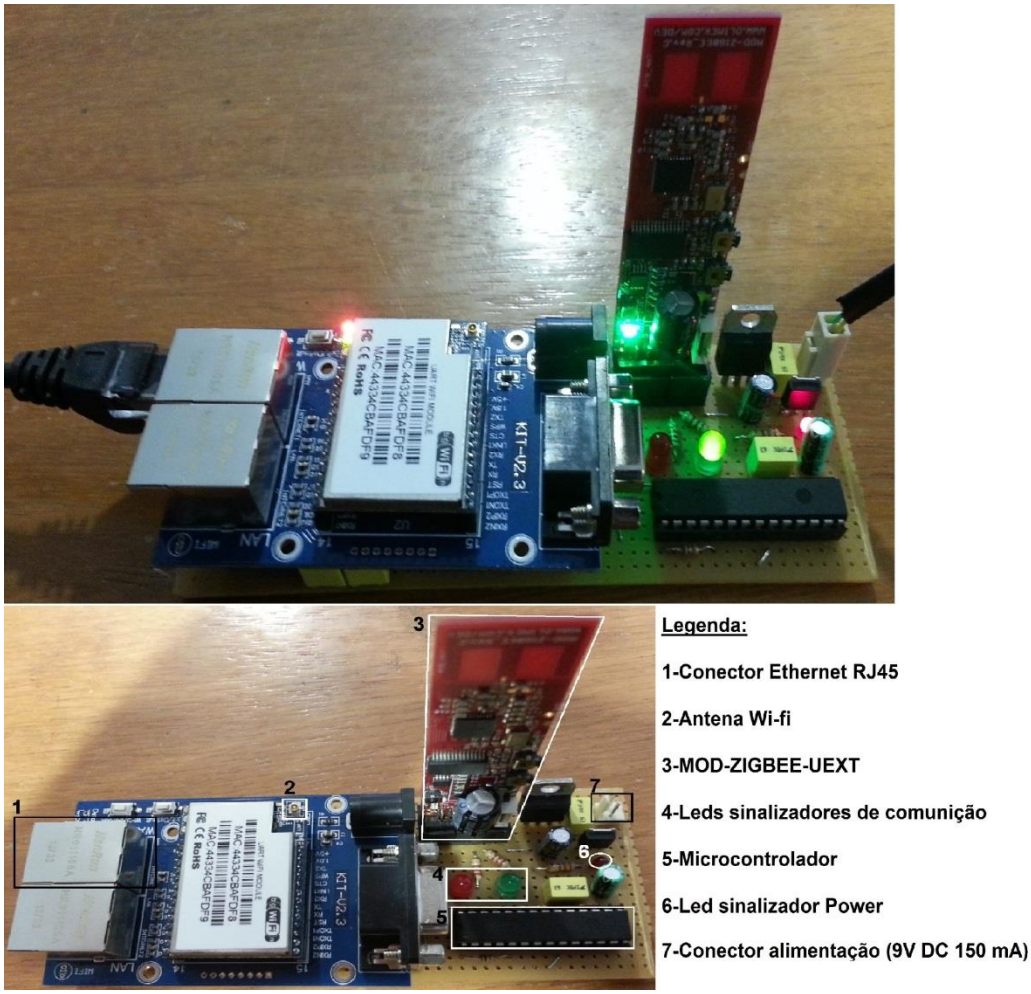


Figura 4.20: módulo central de validação de acesso a espaços (f.p)

Uma vez que o dispositivo integra o equipamento responsável pelo estabelecimento da rede Zigbee (equipamento Zigbee configurado como coordenador), os dispositivos de identificação só poderão comunicar com ele após a rede estar estabelecida e os equipamentos configurados como dispositivos terminais constituintes dos dispositivos de identificação se encontrarem devidamente conectados. Após alimentação do dispositivo, o equipamento Zigbee irá formar a rede e esperar pelos pedidos de conexão de equipamentos terminais garantindo a associação de dispositivos de identificação a este módulo. O *led* de sinalização verde constituinte do dispositivo irá acender quando o correto funcionamento do mesmo estiver garantido.

Quando um pedido de validação de acesso for efetuado, este módulo receberá a mensagem enviada pelo respetivo dispositivo de identificação, com estrutura idêntica à representada pela figura 4.16. A receção da mensagem é efetuada pelo equipamento Zigbee constituinte, sendo remetida para o microcontrolador constituinte do módulo. O

microcontrolador irá processar a informação convertendo-a para uma mensagem HTTP POST, enviando-a posteriormente para o servidor. Uma vez que a comunicação com o servidor recorre à rede internet, é necessário que o módulo admita estabelecer comunicação TCP/IP (45). Esta capacidade é atribuída ao módulo pela integração do equipamento conversor RS-232 to TCP/IP. Este admite conexão com a rede através de uma ligação Ethernet, recorrendo ao conector RJ45, ou através de uma ligação Wi-Fi. A figura 4.21 apresenta o equipamento anunciado.

Figura 4.21: conversor RS-232 to TCP/IP (Ethernet e Wi-fi) (58)

Após processada a informação por parte do servidor, este retorna uma resposta em formato HTML segundo o mesmo protocolo (HTTP) para o módulo. Recebida pelo microcontrolador, este irá processar a informação, compondo uma mensagem de resposta, de estrutura semelhante à representada na figura 4.17, que enviará para o dispositivo de identificação respetivo. A figura 4.22 apresenta um diagrama de comunicação do módulo central de validação de acesso a espaços.

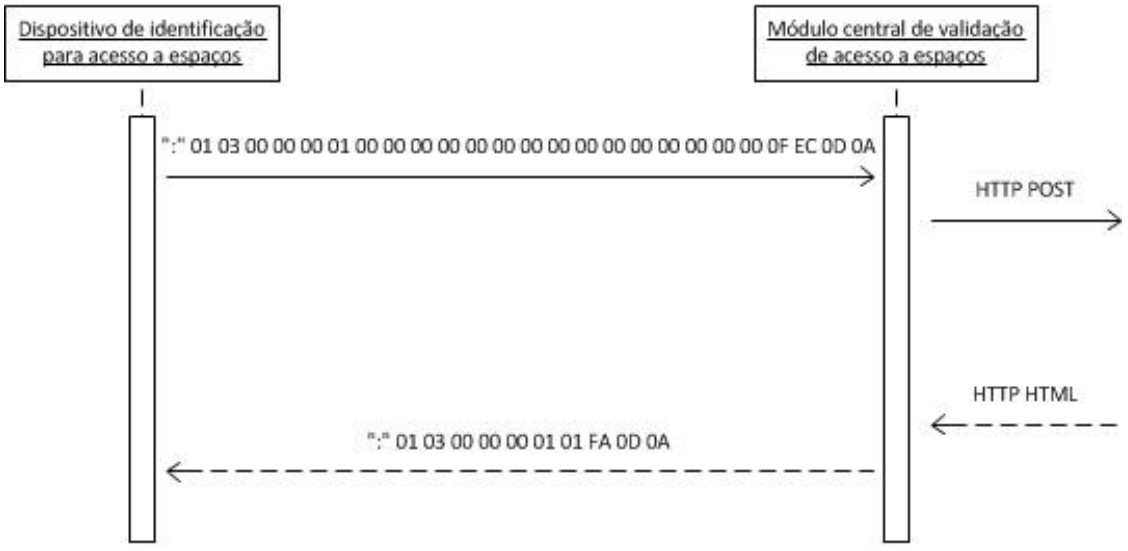


Figura 4.22: diagrama de comunicação do módulo (f.p)

No caso de um pedido ser efetuado ao servidor e este não retorne uma mensagem válida, por falha na ligação ou por falha no processo, o microcontrolador do módulo irá identificar o erro e retornar ainda assim uma mensagem para o dispositivo de identificação respetivo. Esta mensagem será por esse dispositivo interpretada e possibilitará informar o utilizador do erro sucedido, através dos *leds* sinalizadores. Esta mensagem de erro é retornada para esse dispositivo caso uma mensagem não seja enviada pelo servidor até 700ms após o envio do pedido realizado pelo módulo.

Conversor RS-232 to TCP/IP

Este equipamento possibilita a conversão de mensagens entre protocolos. Possibilitando somente a ativaçao simultânea de duas interfaces de comunicação, este equipamento pode comportar-se como conversor RS-232 to TCP/IP Wi-Fi, RS-232 to TCP/IP Ethernet e ainda Wi-Fi to Ethernet (AP). Possibilita funcionamento como servidor TCP e cliente UDP e TCP. Para além destas caracteristicas, admite endereçamento *IP* estático configurado e endereçamento automático por DHCP.

O funcionamento correto deste equipamento depende da adequada configuração necessária. Este equipamento permite que a configuração seja efetuada por qualquer uma das interfaces de comunicação que se encontrem ativas. A configuração com recurso à interface de comunicação RS-232 é efetuada por comandos AT. Por outro lado, a configuração pelas interfaces de comunicação Ethernet e Wi-Fi é efetuada através de uma página web integrada na memória do dispositivo e acessível quando requerida comunicação com este, por tais interfaces. A figura 4.23 apresenta a página de configuração do equipamento.

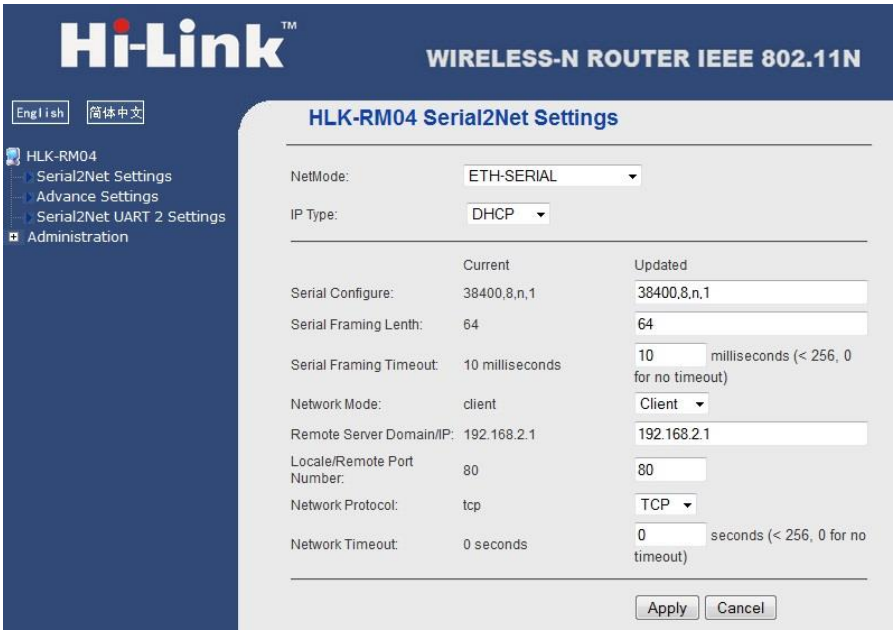


Figura 4.23: interface Web de configuração do equipamento (58)

Como é possível verificar, o equipamento possibilita a configuração de diversas características, tais como, tipologia do conversor, metodologia de endereçamento, parâmetros de comunicação RS-232, tamanho dos mensagens da comunicação serie, tempo expiração da comunicação, endereço IP do dispositivo com o qual deverá estabelecer comunicação TCP (servidor), porta de conexão com o mesmo, modo de funcionamento e tempo de expiração da conexão TCP. No exemplo ilustrado, a metodologia de endereçamento está configurada por DHCP. Caso não o estivesse, seria necessário configurar para além das especificações descritas, o endereço IP, a máscara da rede e ainda o *Default Gateway*.

4.1.4.4 Comunicação alternativa entre dispositivos

Após a implementação dos dois dispositivos constituintes do sistema de validação de acessos a espaços, o autor verifica que a tecnologia de comunicação sem fios implementada (Zigbee) demonstra-se funcional e vantajosa pelo desprendimento de um conjunto de requisitos quando comparada a tecnologias de comunicação por cabo, contudo, em cenários específicos de instalação do sistema poderia apresentar ligeiros desajustes. O autor realça esta questão pela possibilidade de, em determinadas instalações, encontrarem-se acessíveis infraestruturas cabladas junto às portas de acesso aos espaços, cuja finalidade seria estabelecer uma rede de comunicação necessária a sistemas deste tipo. Neste cenário hipotético, a instalação de um sistema sem fios como o concebido neste trabalho seria ainda assim uma excelente aposta,

contudo poderia representar custos desnecessários. Se os dispositivos admitissem, para além da capacidade de comunicação sem fios, a capacidade de conexão a infraestruturas de comunicação cablada, os equipamentos de comunicação Zigbee poderiam ser dispensados, reduzindo o custo total do sistema. Com base nesta abordagem, o autor verificou que o mercado disponibiliza módulos de conversão RS-232 to RS-485 (figura 4.24) e estes admitem compatibilidade física de conexão com os atuais conectores UEXT, constituintes dos dispositivos e responsáveis por conectar os módulos Zigbee.

Figura 4.24: Mod-RS485 Olimex (59)

Estando disponíveis nos conectores dos dispositivos a alimentação e os terminais de comunicação serie, somente seria necessário a disponibilidade de duas interfaces digitais do microcontrolador nestes conectores. Estas possibilitariam o controlo funcional dos equipamentos referidos. O autor verificou que, mesmo possibilitando as duas interfaces digitais nos referidos conectores, nenhuma situação de incompatibilidade seria arrecadada para o atual funcionamento do sistema, dado que os terminais necessários não se encontram atualmente conectados ou em utilização. Por este motivo, e não sendo uma alteração considerada dispendiosa, o autor propôs que estas condições físicas fossem garantidas.

Uma vez que a capacidade de comunicação dos dispositivos, com recurso a uma rede RS-485 (45), não depende somente destas condições físicas, o sistema atualmente não admite comunicação por este meio. Para tal seriam necessárias reconfigurações algorítmicas dos processos executados por cada dispositivo, possibilitando assim a compatibilidade funcional com uma rede de comunicação do tipo enunciada. Sendo a restruturação um processo complexo, a sua execução arrecadaria custos acrescidos para o sistema, sendo necessário ponderar a sua exequibilidade. O autor não avançou com o trabalho neste sentido, uma vez que considerou que o número de cenários, semelhantes ao referido, será reduzido, contudo não desprezou a potencialidade acrescida que o sistema poderia angariar com a compatibilidade de duas tecnologias de comunicação distintas.

4.2 Software

O funcionamento global do sistema, para além dos requisitos de *hardware* que possibilitam uma interação física, depende de software responsável por possibilitar a execução de um conjunto de processos. Este é constituído por um conjunto de aplicações de interação com o utilizador em ambiente gráfico juntamente com algoritmos background de processamento. Enquanto as aplicações são percetíveis para o utilizador pela necessária interação com este, os algoritmos de processamento (*Scripts*) não são percetíveis, contudo o funcionamento do sistema depende da correta integração destes.

Distintamente serão abordados tanto os algoritmos de processamento como as aplicações de interação com o utilizador.

4.2.1 Scripts

Os scripts referem, tal como enunciado anteriormente, algoritmos de processamento background. Com recurso a estes é possível cumprir tarefas necessárias ao correto funcionamento do sistema tais como recolher, inserir e validar informação.

Uma vez que a execução dos processos previstos por estes algoritmos serão centrais, ou seja, requeridos por diversos dispositivos do sistema, os scripts devem ser alojados e posteriormente executados por um dispositivo comum a todo ele. Admitindo a arquitetura centralizada, estes deverão ser alojados e executados pelo servidor. Uma vez que a comunicação entre os dispositivos cliente e servidor é efetuada segundo o protocolo TCP/IP, a transmissão de mensagens responsáveis por definir variáveis processuais será garantida por HTTP. Dadas as condições descritas, a linguagem processual que melhor responde às condições é PHP (60).

O sistema integra dois *scripts*, sendo que um admite a responsabilidade do processamento de validações de permissão de acessos a espaços e o outro do processamento do relógio e calendário universal do sistema.

4.2.1.1 Processamento de validações de permissão de acesso

O processamento deste script depende de duas variáveis de entrada não nulas. Estas variáveis referem o código de identificação do espaço e o código do cartão de identificação, as quais, são recebidas através de um método POST efetuado pelo módulo central de validação de acesso a espaços. Caso ambas, ou uma das variáveis não assuma qualquer valor, o processo executado por este script não decorrerá dada a insuficiente informação necessária.

O processo executado por este script pode ser dividido em dois subprocessos, ou seja, validação da permissão e registo do acontecimento no sistema. O subprocesso que decorre primeiramente é o de validação, o qual consiste em identificar o utilizador através do código do cartão e seguidamente recolher da base de dados informação que confirme a permissão deste utilizador ao respetivo espaço. Caso esta se verifique, uma segunda validação deverá decorrer de modo a confirmar se a hora e data atuais respeitam o intervalo definido pela hora e data de início e término da permissão de acesso. Caso esta seja novamente verificada, será retornada uma resposta em formato HTML para o respetivo cliente (módulo central de validação de acesso a espaços) com indicação de permissão. Caso uma destas condições não seja verificada, a mensagem retornada é idêntica porém contendo a negação ao acesso.

Após o envio da resposta, o segundo subprocesso é iniciado, ou seja, é inserida a informação referente na base de dados, registando deste modo a permissão ou negação do acesso pelo utilizador ao respetivo espaço.

4.2.1.2 Processamento do calendário e relógio do sistema

Sendo o sistema constituído por um conjunto indeterminado de dispositivos que possibilitam o registo de acontecimentos e procedimentos, os quais devem ser temporalmente definidos, é necessário garantir que esta informação temporal seja coerente. Não sendo possível garantir que os relógios e calendários locais de cada um dos dispositivos estejam devidamente sincronizados, é requerido o acesso a um relógio e calendário comuns a todos eles. Sendo o processamento do script realizado pelo servidor, a informação temporal será baseada no relógio e calendário deste.

O processamento do script depende de uma variável de entrada não nula. O processo e posterior resposta dependem do valor desta variável, podendo esta assumir três distintos valores. De acordo com ele, a resposta poderá conter informação do relógio, do calendário ou de ambos.

4.2.2 Aplicações de interação com o sistema de informação

As aplicações referem interfaces que possibilitam a gestão das variáveis do sistema. Pela necessária interação com o utilizador, estas aplicações decorrem em ambiente gráfico de modo a que a interface seja intuitiva e de prática utilização. As aplicações decorrem em qualquer dispositivo *Desktop* e *Laptop* que integre um sistema operacional Microsoft, ou seja, Windows Vista, Windows 7 ou Windows 8. Esta situação deve-se ao facto das aplicações estarem desenvolvidas em plataforma Visual Studio, em linguagem Visual Basic (61).

O sistema integra um conjunto de sete aplicações cujas funções são distintas. A não inclusão de todas as aplicações numa única justifica-se pela desnecessária integração de funcionalidades que os utilizadores poderão não ter acesso. Sendo a dinâmica funcional do sistema centrada no utilizador, as funcionalidades a que poderão ter permissão de acesso variam de acordo com o estatuto associado a cada um deles. Os acessos às aplicações destinam-se somente a utilizadores de gerência, ou seja, cujos estatutos sejam diferentes de "Cliente", pelo que não será possível a interação destes utilizadores com qualquer aplicação.

A interação com as aplicações depende ainda do prévio processo de identificação e autenticação nestas, sendo este possível através de credenciais (*Username* e *Password*). Por uma questão de padronização, a interface inicial (*Login*) de cada uma das aplicações é idêntica, podendo estas ser distinguidas pelo nome em título (figura 4.25).

Figura 4.25: interface genérica de Login (f.p)

O campo de preenchimento referente à *Password* não permite a visualização da mesma. Por questões de segurança, no processo de *login,* a *Password* é encriptada segundo o algoritmo de encriptação unidirecional MD5 (62), impossibilitando a captação desta.

Dado que as aplicações necessitam interagir com o servidor pela necessária requisição e registo de dados, incluindo o processo de *login*, os dispositivos que as integram devem admitir capacidade de interação remota com a base de dados, sendo imposto a necessária conexão do respetivo dispositivo à rede Internet. Para além deste requisito, o dispositivo deverá estar dotado com um Software de interface (ODBC) necessário à comunicação entre as aplicações e a base de dados. (MySQL Connector) (63).

4.2.2.1 Gestor de logins

Esta aplicação tem como objetivo possibilitar a gestão dos acessos às aplicações permitidas a cada utilizador. As atribuições de acesso editáveis a cada utilizador do sistema variam de acordo com o seu estatuto. A figura 4.26 demonstra alguns cenários gráficos da aplicação em questão.

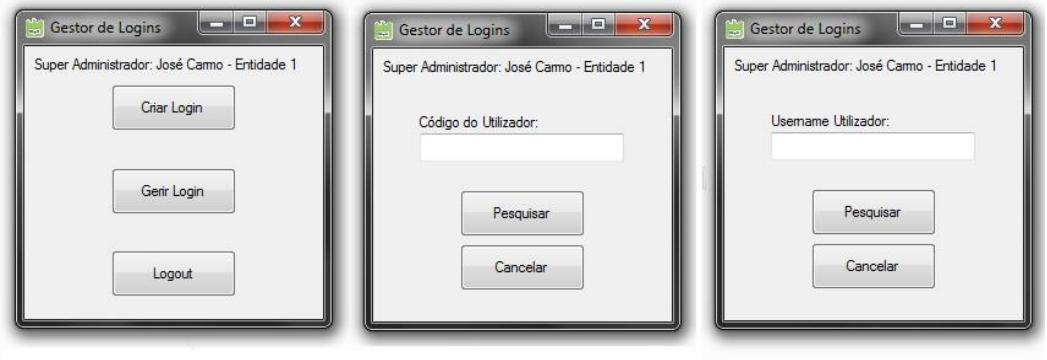


Figura 4.26: interface de pesquisa das duas funcionalidades (f.p)

Para possibilitar o acesso às aplicações é necessário que ao utilizador estejam associadas as respetivas credenciais de acesso (*Username* e *Password*), pelo que também é objetivo desta aplicação poder registá-las (figura 4.27).

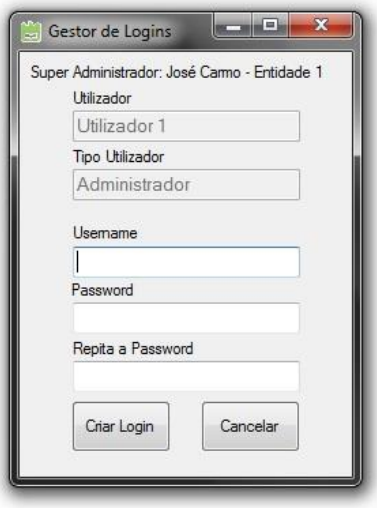


Figura 4.27: interface de registo de credenciais (f.p)

O acesso a esta aplicação, por questões de segurança, somente é possível atribuir a utilizadores com estatutos de "Super Administrador" e "Administrador", sendo que as

funcionalidades disponíveis variam de acordo com estes. A aplicação possibilita as seguintes funcionalidades de acordo com o estatuto do utilizador desta:

1. Estatuto "Super Administrador" (figura 4.28):
    - Criar credenciais de acesso (*Logins*) às aplicações para qualquer utilizador;
    - Gerir as permissões de acesso às aplicações para qualquer utilizador;
    - Definir os espaços que cada utilizador pode gerir através da aplicação para o efeito (Gestor de Espaços);
    - Definir os serviços que cada utilizador pode atribuir acesso, através da aplicação para o efeito (Gestor de Serviços);
    - Definir os serviços que cada utilizador poderá prestar (validar o acesso) através da aplicação para o efeito (Gestor de Serviços);
    - Remover credenciais de acesso a qualquer utilizador;

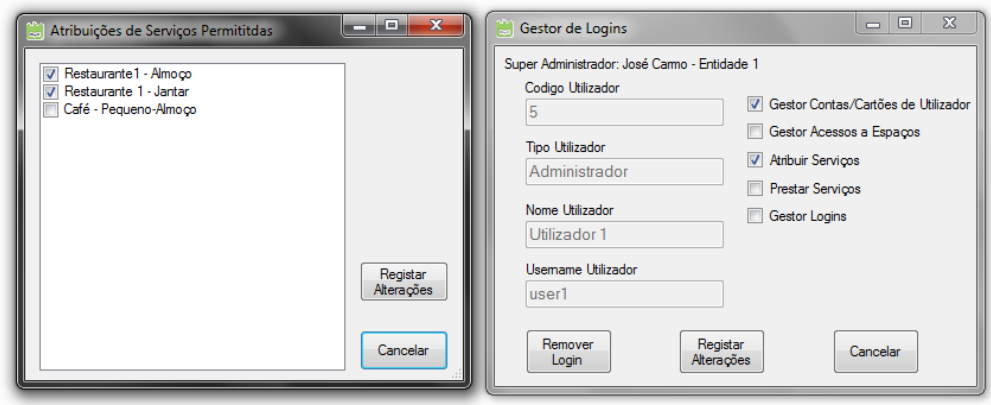
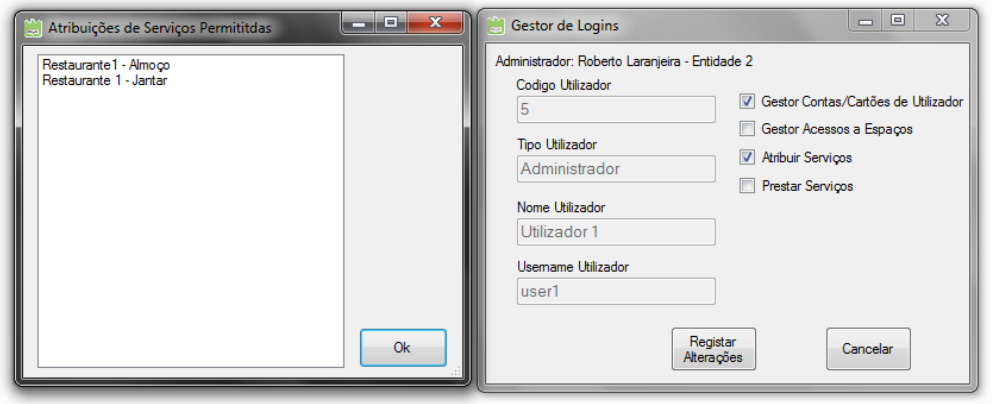


Figura 4.28: interface da aplicação para utilizadores de estatuto "Super Administrador" (f.p)

2. Estatuto "Administrador" (figura 4.29):
    - Criar credenciais de acesso às aplicações para utilizadores de estatuto diferente de "Super Administrador" e cuja entidade associada seja igual à que pertence;
    - Gerir as permissões de acesso às aplicações para qualquer utilizador cujo estatuto seja diferente de "Super Administrador" e a entidade à qual se encontra associado seja igual à que pertence;
    - Consultar os espaços que cada utilizador pode gerir, através da aplicação para o efeito (Gestor de Espaços), cujo estatuto seja diferente de "Super

Administrador" e a entidade à qual se encontra associado seja igual à que pertence;

- Consultar os serviços que cada utilizador pode atribuir acesso, através da aplicação para o efeito (Gestor de Serviços), cujo estatuto seja diferente de "Super Administrador" e a entidade à qual se encontra associado seja igual à que pertence;
- Consultar os serviços que cada utilizador pode prestar (validar o acesso) através da aplicação para o efeito (Gestor de Serviços), cujo estatuto seja diferente de "Super Administrador" e a entidade à qual se encontra associado seja igual à que pertence.



igura 4.29: interface da aplicação para utilizadores de estatuto "Administrador" (f.p)

4.2.2.2 Administrador de serviços

Esta aplicação possibilita a gestão dos registos de serviços no sistema, ou seja, permite registar novos serviços e alterar dados de serviços já registados. Uma vez que admite funcionalidades de manutenção do sistema, o acesso a esta aplicação é somente possível atribuir a utilizadores de estatuto "Super Administrador".

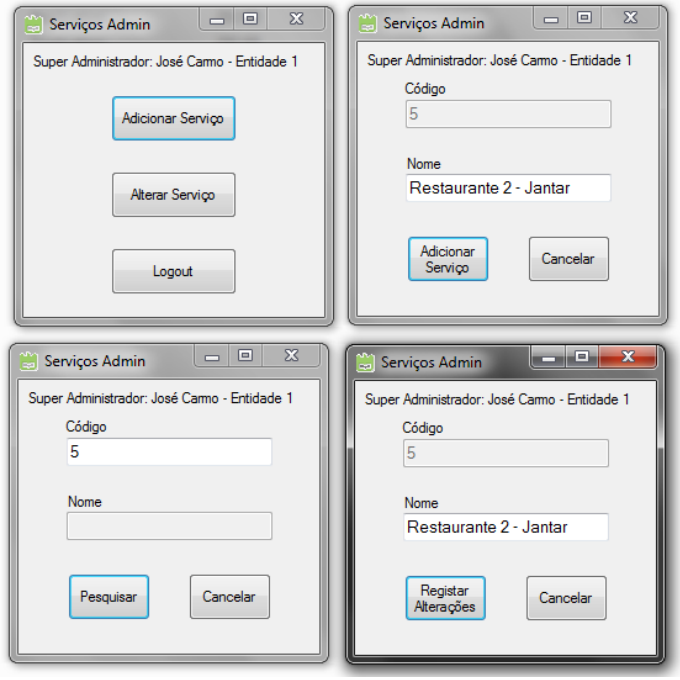


Figura 4.30: interface da aplicação administrador de serviços (f.p)

Como é possível verificar pela figura 4.30, o código do serviço é atribuído automaticamente quando um novo registo for efetuado pelo que, nunca é possível ao utilizador editá-lo. O utilizador somente pode atribuir e modificar posteriormente o nome de identificação de cada serviço.

A pesquisa necessária ao processo de alteração pode ser efetuada por nome ou pelo código do serviço.

4.2.2.3 Administrador de espaços

Esta aplicação, tal como a anterior, integra funcionalidades referentes a manutenção, pelo que, o acesso é somente possível atribuir a utilizadores de estatuto "Super Administrador". Esta tem por objetivo possibilitar a gestão dos registos de espaços no sistema, ou seja, permite registar novos espaços e alterar dados de espaços já registados.

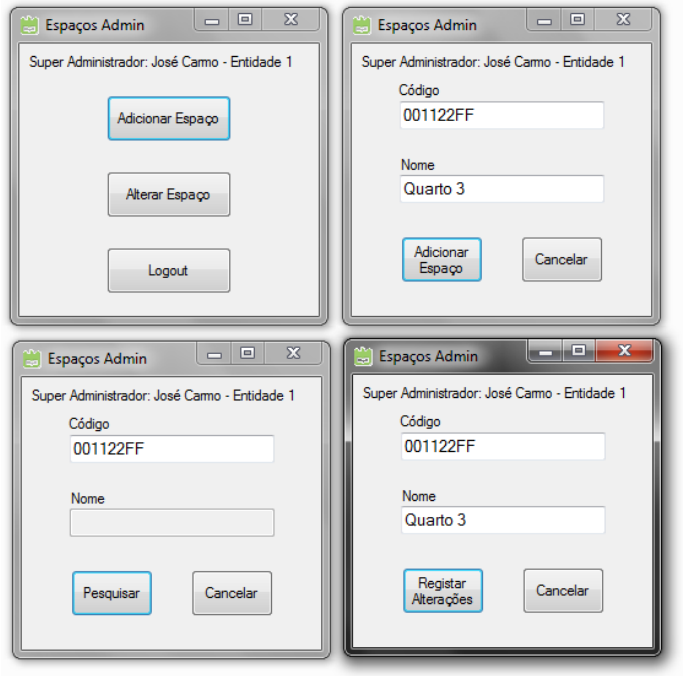


Figura 4.31: interface da aplicação administrador de espaços (f.p)

Contrariamente à aplicação anterior, tanto o código como o nome do espaço devem ser inseridos manualmente pelo utilizador no processo de um novo registo (figura 4.31). O código a inserir manualmente é composto por oito caracteres que representam o valor hexadecimal de quatro bytes, definido no respetivo dispositivo de identificação para acesso a espaços instalado junto à porta respetiva. Uma vez que o registo de espaços pode ser efetuado sem uma ordem sequencial dos dispositivos, a inserção automática do código constituiria um problema para o registo dos mesmos. Apesar do código ser inserido manualmente, o sistema impossibilita a repetição de códigos de registo, evitando redundâncias incoerentes.

No processo de alteração de um registo é possível reconfigurar o código e o nome do espaço, sendo que a pesquisa prévia pode ser efetuada de igual modo por código ou por nome do espaço.

4.2.2.4 Administrador de entidades

Esta aplicação tem por objetivo possibilitar a gestão dos registos das entidades no sistema. O acesso a esta, tal como nas duas anteriores, é possível atribuir a utilizadores de estatuto “Super Administrador”, porque integra de igual modo funcionalidades de manutenção do sistema. Através desta aplicação é possível registar novas entidades e alterar dados de entidades já registadas.

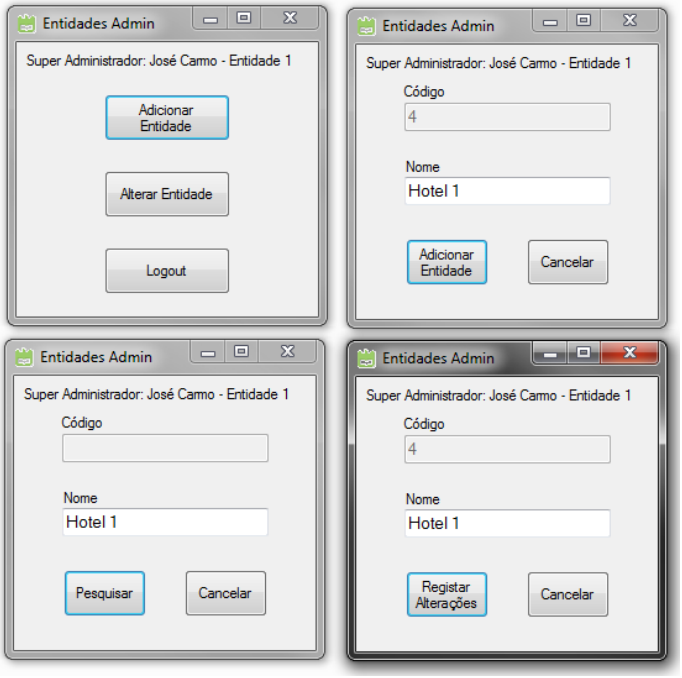


Figura 4.32: interface da aplicação administrador de entidades (f.p)

Esta aplicação, tal como demonstra a figura 4.32, admite um funcionamento global semelhante à aplicação "Administrador de Serviços", contudo é referente a entidades.

4.2.2.5 Gestor de Contas e Cartões de Utilizador

Esta aplicação tem como objetivo possibilitar a gestão de informações referentes aos utilizadores, e permitir a associação de etiquetas RFID aos respetivos utilizadores. Deste modo, a aplicação possibilita o registo de utilizadores, a alteração de dados dos mesmos e associação de etiquetas a utilizadores específicos.

Uma vez que a aplicação integra funcionalidades relacionadas com as etiquetas RFID, é implícita a necessária conexão de um dispositivo de leitura e escrita de etiquetas RFID ao respetivo computador de modo a possibilitar o acesso a todas as funcionalidades da aplicação. A figura 4.33 apresenta a interface da aplicação descrita.

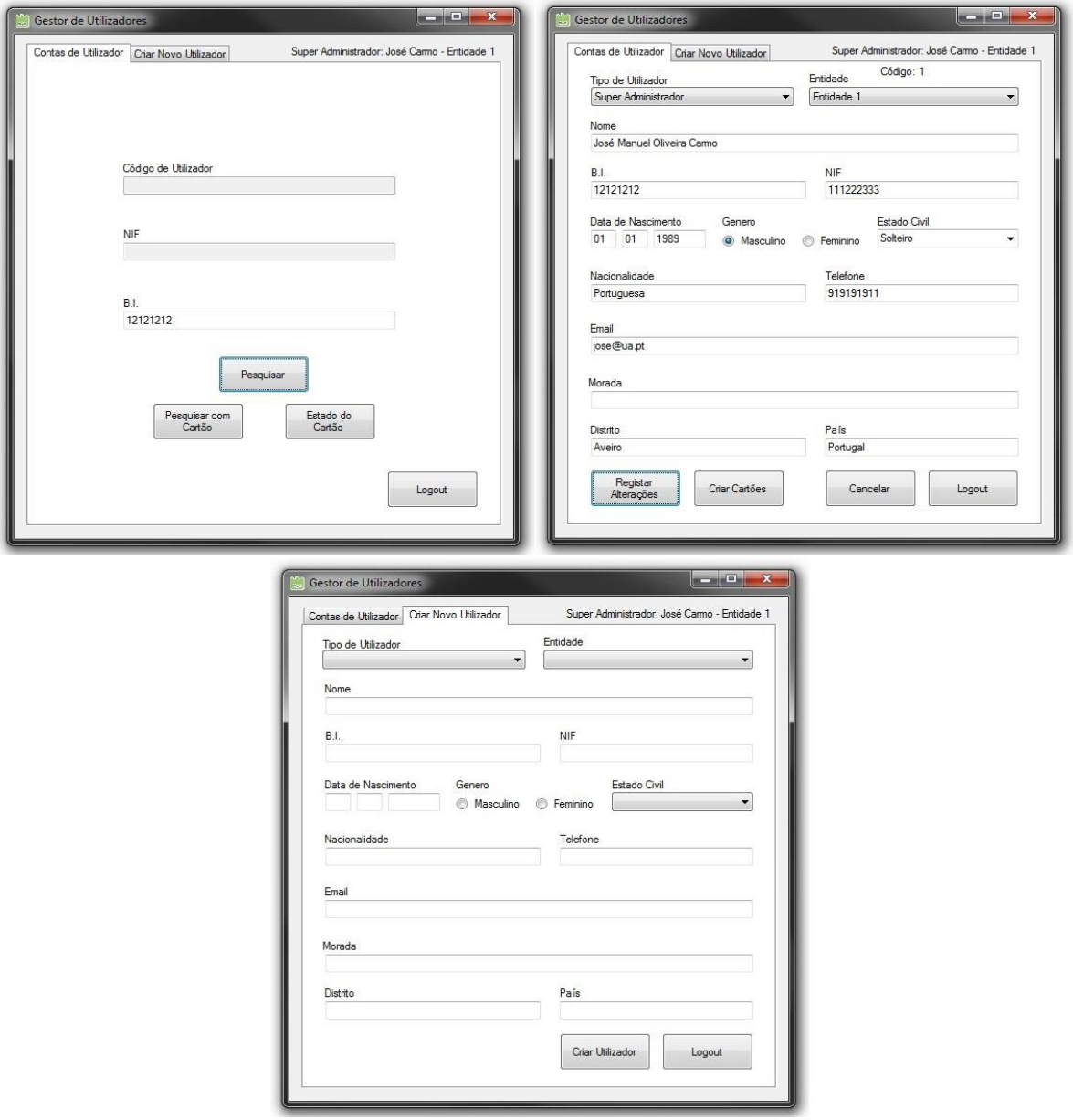


Figura 4.33: interface de gestão de contas e de etiquetas de utilizador (f.p)

O acesso a esta aplicação é possível a utilizadores cujo estatuto seja diferente de "Cliente", contudo as funcionalidades disponíveis variam de acordo com o estatuto do mesmo, sendo disponíveis as seguintes funcionalidades de acordo com cada um deles:

1. Estatuto "Super Administrador":
    - Registar novos utilizadores, podendo associá-los a qualquer entidade registada no sistema e atribuir-lhe qualquer um dos quatro estatutos admitidos;

- Aceder a toda a informação de qualquer utilizador registado no sistema, através de identificação por etiqueta ou por pesquisa de dado exclusivo, com possibilidade de alteração de qualquer um dos dados;
- Associar nova etiqueta a qualquer utilizador cujos dados foram acedidos;
- Replicar etiqueta associada ao utilizador cujos dados foram acedidos;
- Verificar estado de qualquer etiqueta face ao sistema, desde que compatível com os dispositivos de interação.

2. Estatuto "Administrador":
    - Registar novos utilizadores, podendo atribuir-lhes qualquer um dos estatutos exceto "Super Administrador", ficando o utilizador automaticamente associado à mesma entidade do utilizador da aplicação;
    - Aceder a toda a informação de qualquer utilizador registado no sistema e cujo estatuto seja "Cliente", através de identificação por etiqueta ou por pesquisa de dado exclusivo;
    - Possibilidade de alteração de todos os dados de utilizadores, exceto a entidade associada e atribuição de estatuto "Super Administrador", cujo estatuto seja "Cliente" e cuja entidade associada seja igual à que pertence;
    - Aceder a toda a informação de qualquer utilizador registado no sistema, cujo estatuto seja "Colaborador" e "Administrador" e a entidade associada seja igual à que pertence, através de identificação por etiqueta ou por pesquisa de dado exclusivo;
    - Possibilidade de alteração de todos os dados de utilizadores, exceto entidade associada e atribuição de estatuto "Super Administrador", cujo estatuto seja "Colaborador" e "Administrador" e cuja entidade associada seja igual à que pertence;
    - Associar nova etiqueta a qualquer utilizador cujos dados foram acedidos e cuja entidade associada seja igual à que pertence;
    - Replicar etiqueta associada ao utilizador cujos dados foram acedidos e cuja entidade associada seja igual à que pertence;
    - Verificar estado de qualquer etiqueta face ao sistema, desde que compatível com os dispositivos de interação.

3. Estatuto "Colaborador":
    - Registar novos utilizadores podendo atribuir-lhe somente estatuto "Cliente", ficando este associado à mesma entidade do utilizador da aplicação;
    - Aceder a toda a informação de qualquer utilizador registado no sistema, cujo estatuto seja "Cliente", através de identificação por etiqueta, e alteração da entidade associada caso seja diferente da entidade do utilizador da aplicação;
    - Aceder a toda a informação de qualquer utilizador registado no sistema cujo estatuto seja "Cliente" e entidade associada seja igual à que pertence, através de pesquisa por dado exclusivo;
    - Possibilidade de alteração de todos os dados, exceto estatuto e entidade associada quando a entidade associada ao utilizador seja igual à que pertence;
    - Associar nova etiqueta a qualquer utilizador cujos dados foram acedidos e a entidade associada seja igual à que pertence;
    - Replicar etiqueta associada ao utilizador cujos dados foram acedidos a entidade associada seja igual à que pertence;
    - Verificar estado de qualquer etiqueta face ao sistema, desde que compatível com os dispositivos de interação.

4.2.2.6 Gestor de Serviços

Esta aplicação possibilita a atribuição de acessos a serviços e registo de prestação dos mesmos. Permite ainda consultar dados relacionados com a atribuição e prestação dos serviços. Uma vez que as duas funcionalidades (atribuição e prestação) encontram-se reunidas numa só aplicação, o acesso a esta é possível a utilizadores cujo estatuto seja diferente de "Cliente" e os quais tenham pelo menos uma permissão autorizada seja de atribuição ou de prestação. O acesso à funcionalidade de atribuição e respetiva interface de consulta estatística somente é possível se o utilizador estiver autorizado a atribuir acesso a pelo menos um serviço. O mesmo decorre para a prestação, não podendo ser acedida a respetiva interface de registo nem a interface de consulta estatística, caso ao utilizador não esteja permitida a prestação de pelo menos um serviço.

A figura 4.34 apresenta a interface da aplicação exemplificando a atribuição e o registo de prestação.

Figura 4.34: interface da aplicação gestor de serviços (f.p)

Os processos, tanto de atribuição como de registo de prestação dependem da prévia identificação do utilizador respetivo. Por questões de segurança, a identificação do utilizador só poderá ser efetuada com recurso a uma etiqueta RFID. Por esta característica, o funcionamento global da aplicação, tal como a anterior, requer um dispositivo de leitura e escrita de etiquetas devidamente conectado ao computador.

Relativamente à interface de consulta estatística, as informações disponibilizadas, quer referentes a prestações quer referentes a atribuições, variam de acordo com o estatuto do utilizador.

Prestação

Nesta interface de consulta (figura 4.35), o utilizador, de acordo com o seu estatuto, poderá visualizar detalhadamente os registos de prestação efetuados no sistema.

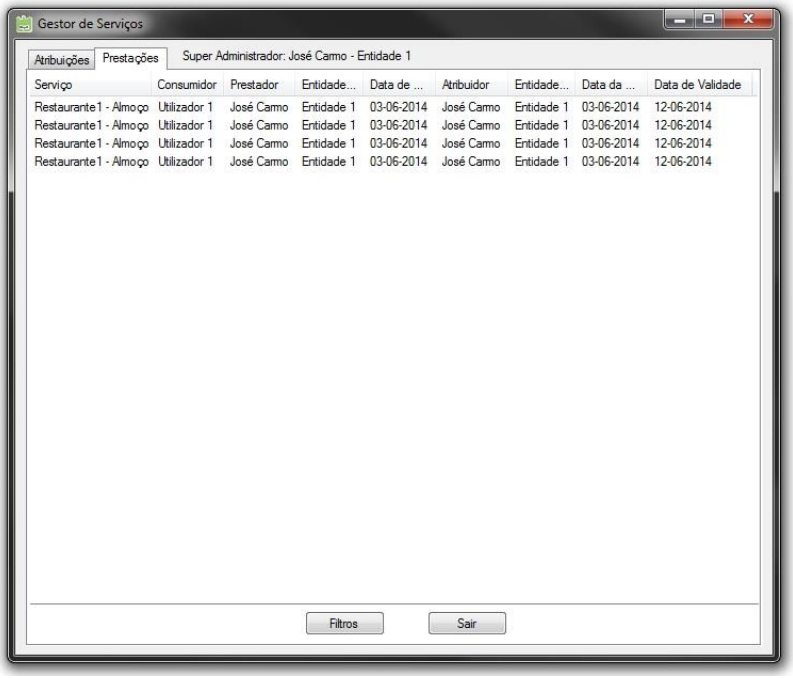


Figura 4.35: interface de consulta dos registos de serviços prestados (f.p)

1. Estatuto "Super Administrador":
    - Acede a todos os registos do sistema associados à prestação de serviços, aos quais, tem permissão de registo de prestação;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador prestador, entidade do utilizador prestador, data da prestação, utilizador atribuidor, entidade do utilizador atribuidor, data da atribuição e data de validade do acesso ao serviço.

2. Estatuto "Administrador":
    - Acede a todos os registos do sistema, associados à prestação de serviços, para os quais tenha permissão de registo de prestação e cujos registos correspondentes foram efetuados por si ou por utilizadores associados à mesma entidade que ele;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador prestador, entidade do utilizador prestador, data da prestação, entidade do utilizador atribuidor, data da atribuição e data de validade do acesso ao serviço.

3. Estatuto "Colaborador"
    - Acede a todos os registos do sistema associados à prestação de serviços, cujos registos correspondentes tenham sido por si efetuados;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador prestador, entidade do utilizador prestador e data de prestação.

Atribuição

Nesta interface de consulta (figura 4.36), o utilizador, de acordo com o seu estatuto, poderá visualizar detalhadamente os registos das atribuições de acesso a serviços efetuadas no sistema.

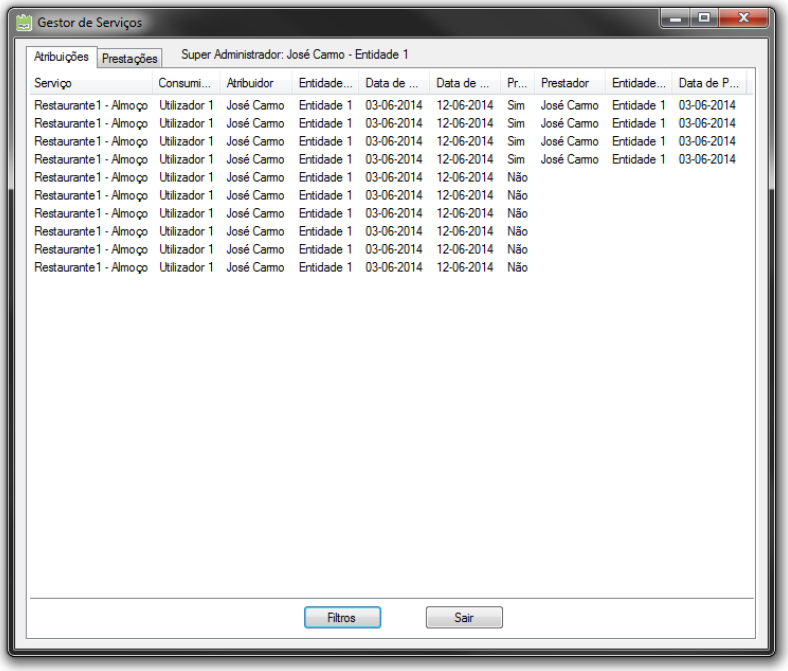


Figura 4.36: interface de consulta dos registos de atribuições de acesso a serviços (f.p)

1. Estatuto "Super Administrador":
    - Acede a todos os registos do sistema associados à atribuição de permissões de acesso a serviços, aos quais tem permissão de atribuição;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador atribuidor, entidade do utilizador atribuidor, data

de atribuição, data de validade do acesso ao serviço, Estado do acesso, utilizador prestador (caso o serviço tenha sido prestado), entidade do utilizador prestador (caso o serviço tenha sido prestado) e data da prestação (caso o serviço tenha sido prestado).

2. Estatuto "Administrador":
    - Acede a todos os registos do sistema associados à atribuição de permissões de acesso a serviços, aos quais tenha permissão de atribuição e cujos registos correspondentes tenham sido efetuados por si ou por utilizadores associados à mesma entidade que ele;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador atribuidor, entidade do utilizador atribuidor, data de atribuição, data de validade do acesso ao serviço, estado do acesso, entidade do utilizador prestador (caso o serviço tenha sido prestado) e data da prestação (caso o serviço tenha sido prestado).

3. Estatuto "Colaborador":
    - Acede a todos os registos do sistema associados à atribuição de permissões de acesso a serviços, cujos registos correspondentes tenham sido por si efetuados;
    - Acede para cada um deles às seguintes informações: serviço, utilizador consumidor, utilizador atribuidor, entidade do utilizador atribuidor, data de atribuição e data de validade do acesso ao serviço.

Uma vez que a quantidade de dados apresentada nestas interfaces pode ser elevada, a aplicação possibilita filtrar dados de acordo com uma ou um conjunto de condições. A interface, que possibilita parametrizar os dados visíveis, é apresentada na figura 4.37.

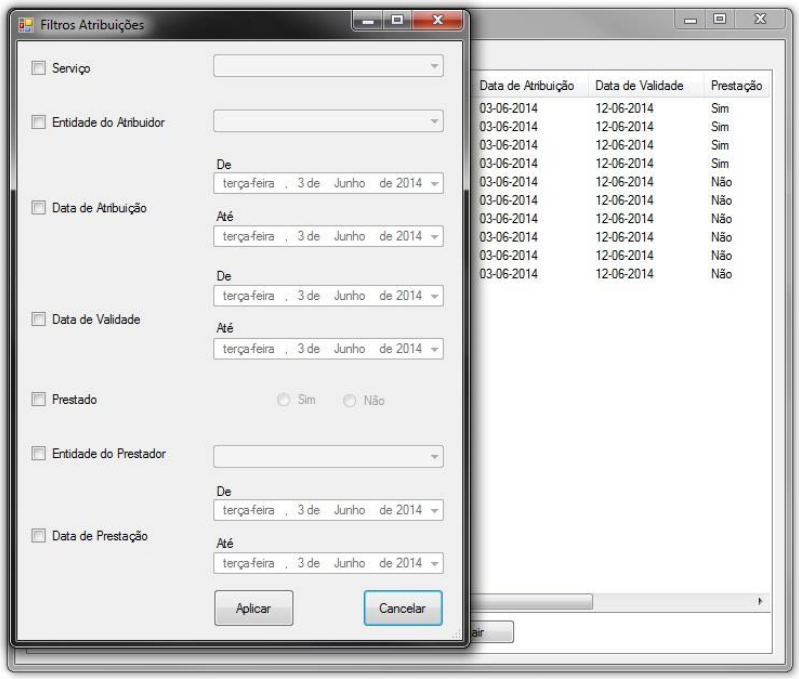


Figura 4.37: interface de parametrização da consulta (f.p)

4.2.2.7 Gestor de Espaços

Esta aplicação tem por objetivo possibilitar a atribuição de permissões de acesso a espaços, bem como possibilitar a análise das atribuições concedidas e ainda consultar o histórico das validações de acesso aos espaços efetuadas pelos utilizadores. Como a anterior, esta aplicação é acessível por utilizadores cujo estatuto seja diferente de "Cliente" e aos quais esteja permitida a atribuição de permissões de acesso a pelo menos um espaço. A figura 4.38 apresenta a interface da aplicação para atribuição de permissão de acesso a espaço.

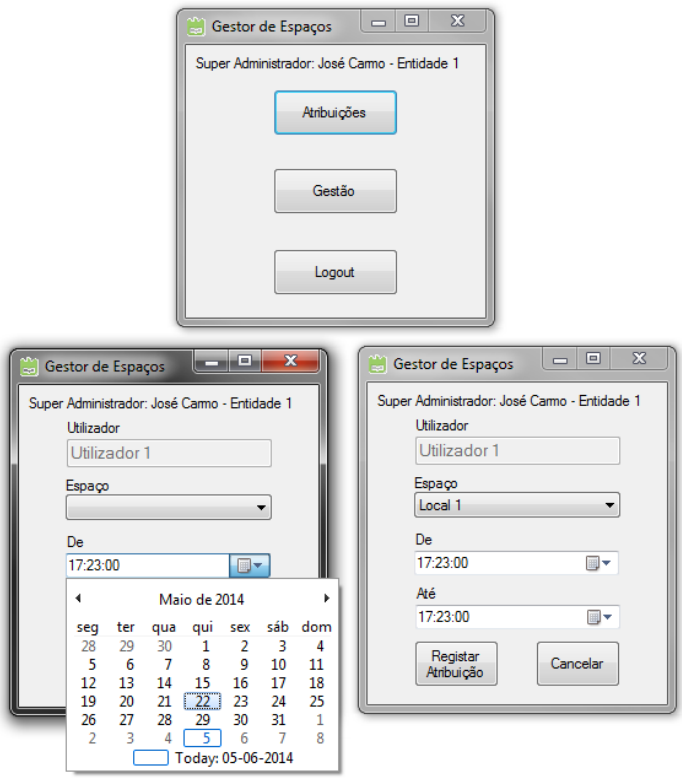


Figura 4.38: interface da aplicação gestor de espaços (f.p)

Como é possível verificar, a atribuição de permissão de acesso a espaço requer a definição das datas e horas de início e término.

A aplicação integra interface de consulta de dados pelo que, as informações disponibilizadas, tal como na anterior aplicação, dependem do estatuto do utilizador da aplicação. A interface de consulta é constituída por duas secções, sendo uma referente aos registos de permissões efetuados e a outra ao histórico de validações efetuadas pelos utilizadores.

Permissões atribuídas

Nesta interface de consulta (ver figura 4.39), o utilizador, dependente do seu estatuto, poderá visualizar detalhadamente os registos de atribuições de acesso efetuados no sistema.

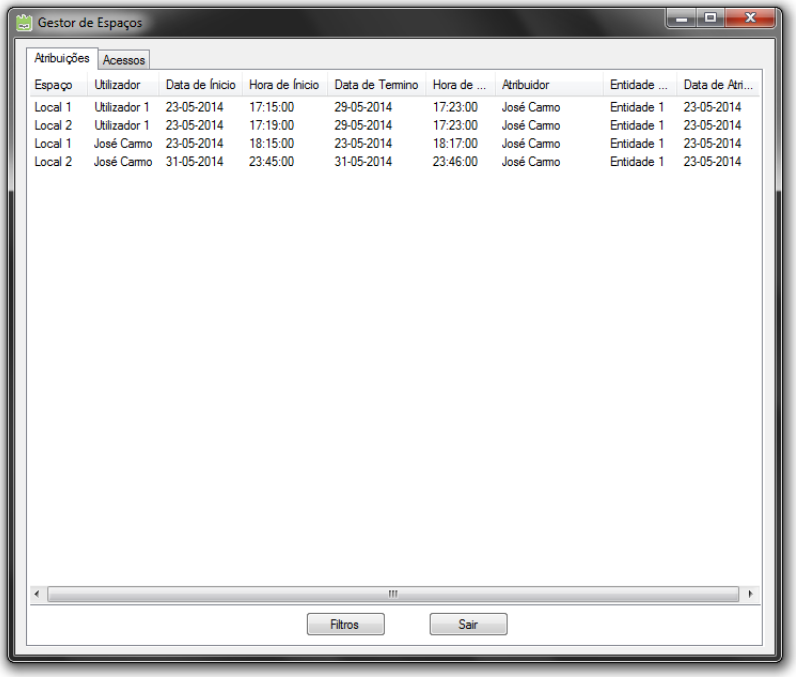


Figura 4.39 interface de consulta das atribuições de acesso a espaços efetuadas (f.p)

1. Estatuto "Super Administrador" e "Administrador":
    - Acede a todos os registos do sistema, referentes a atribuições de permissões de acesso a espaços, aos quais, tem permissão de atribuição;
    - Acede para cada um deles às seguintes informações: espaço, utilizador, data de início, hora de início, data de término, hora de término, utilizador atribuidor, entidade do utilizador atribuidor e data da atribuição.

2. Estatuto "Colaborador":
    - Acede a todos os registos do sistema referentes a atribuições de permissões de acesso a espaços por ele efetuadas;
    - Acede para cada um deles às seguintes informações: espaço, utilizador, data de início, hora de início, data de término, hora de término, utilizador atribuidor, entidade do utilizador atribuidor e data da atribuição.

Validações de acesso realizadas

Nesta interface de consulta (figura 4.40), o utilizador, de acordo com o seu estatuto, poderá visualizar detalhadamente os registos referentes às validações de acesso efetuadas pelos utilizadores.

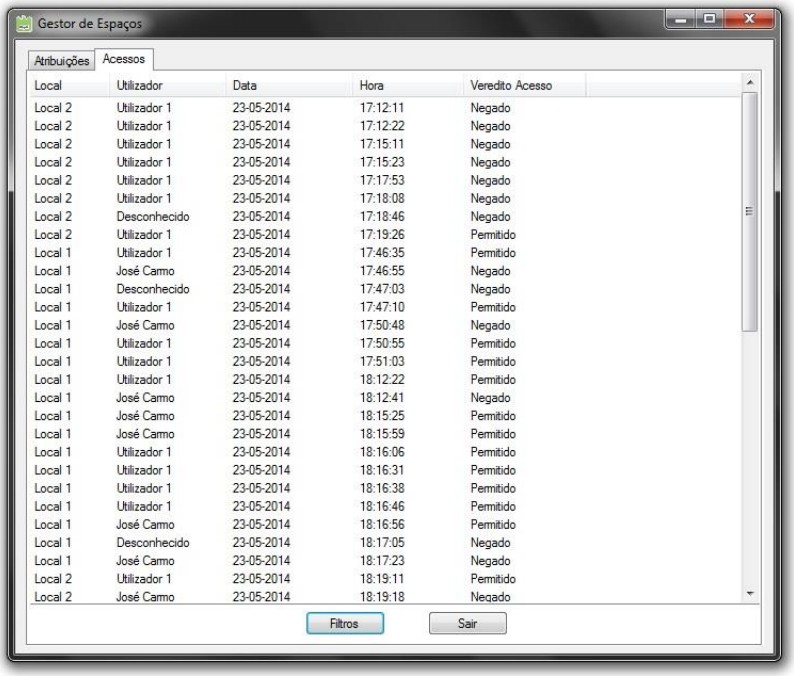


Figura 4.40: interface consulta das validações de acesso a espaços efetuadas (f.p)

1. Estatuto “Super Administrador” e “Administrador”:
    - Acede a todos os registos do sistema associados à validação de acessos a espaços, aos quais tem permissão de atribuição.
    - Acede para cada um deles às seguintes informações: espaço, utilizador, data, hora e veredito.
2. Estatuto “Colaborador”:
    - Não tem acesso a esta interface de consulta.

Tal como a aplicação anteriormente descrita, também possibilita filtrar as informações disponibilizadas de acordo com uma ou um conjunto de condições. A figura 4.41 demonstra a interface que possibilita a parametrização da consulta.

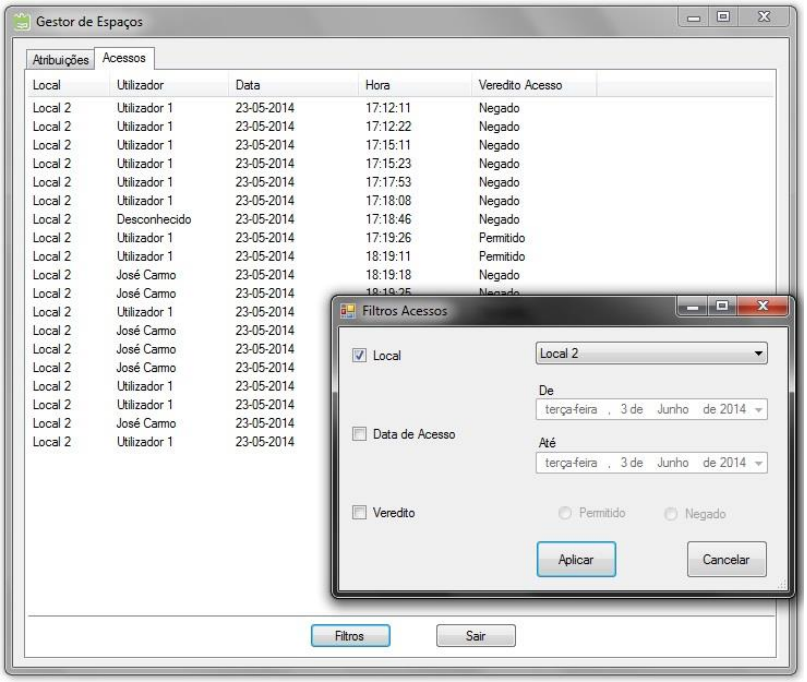


Figura 4.41: interface de parametrização da consulta (f.p)

4.3 Base de Dados

A base de dados é a estrutura de armazenamento responsável por garantir a preservação atualizada de toda a informação necessária ao funcionamento estabelecido para o sistema.

Sendo o acesso à base de dados requerido por qualquer dispositivo do sistema, esta deve estar armazenada num dispositivo comum. Admitindo o sistema uma arquitetura centralizada, a base de dados, tal como os scripts, devem ser alojados pelo servidor.

Reunidas todas as condições do sistema, o autor verifica que o modelo da base de dados, que melhor ajuste apresenta, é MySQL. Admitindo que o servidor do sistema será um servidor web, a compatibilidade com bases de dados deste tipo é garantida.

Sendo o sistema dependente do acesso à informação, o autor reuniu e relacionou os dados que a base de dados deve armazenar e possibilitar acesso para um correto funcionamento do sistema. A figura 4.42 apresenta esquematicamente o conjunto de dados necessários armazenar e o relacionamento entre eles.

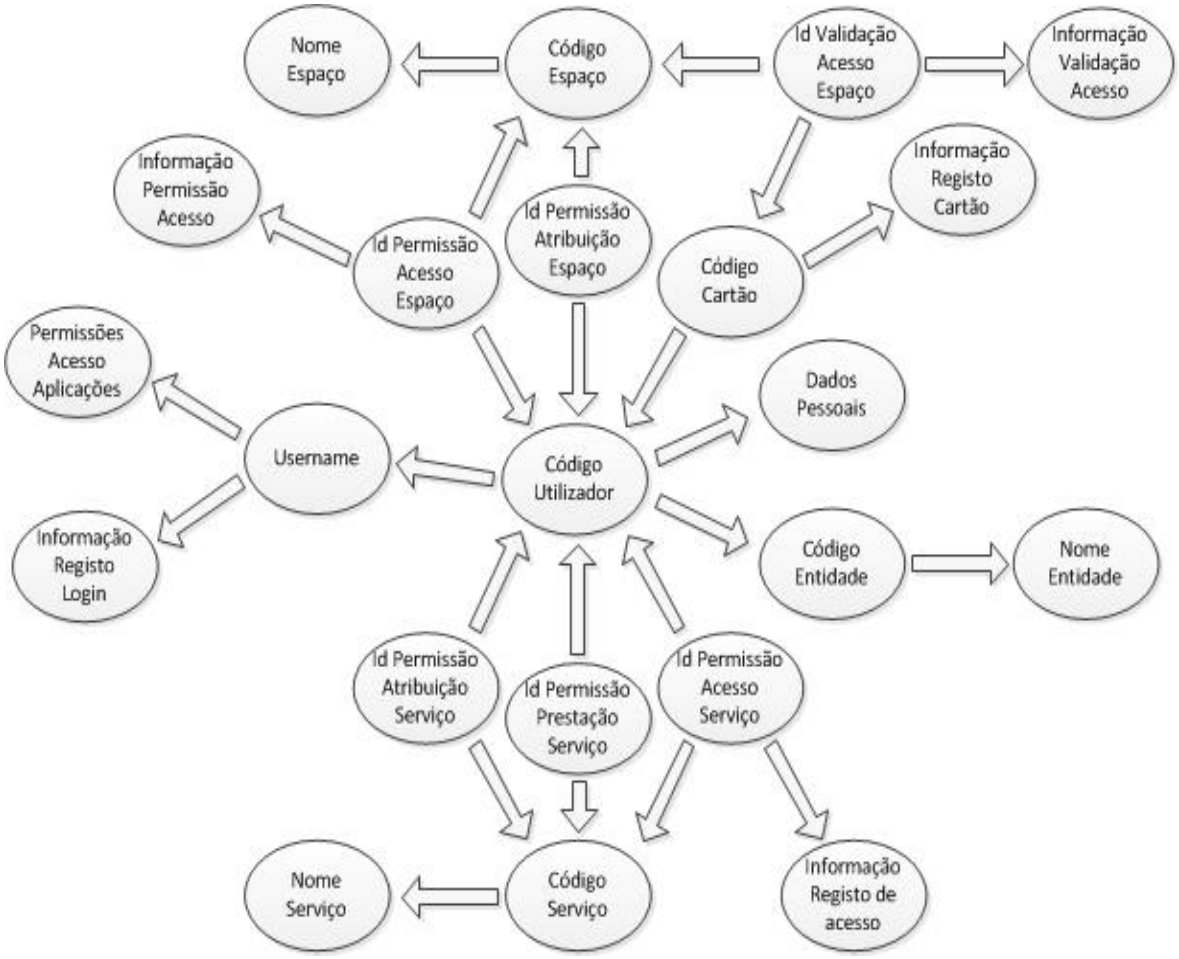


Figura 4.42: dados necessários armazenar e relação entre eles (f.p)

Analisando o conjunto de dados e suas relações, o autor estruturou a base de dados atendendo a forma normal de Boyce-Codd (64). Verificada a normalização, a base de dados constitui-se por 12 tabelas cujo diagrama relacional *UML* é apresentado na figura 4.43.

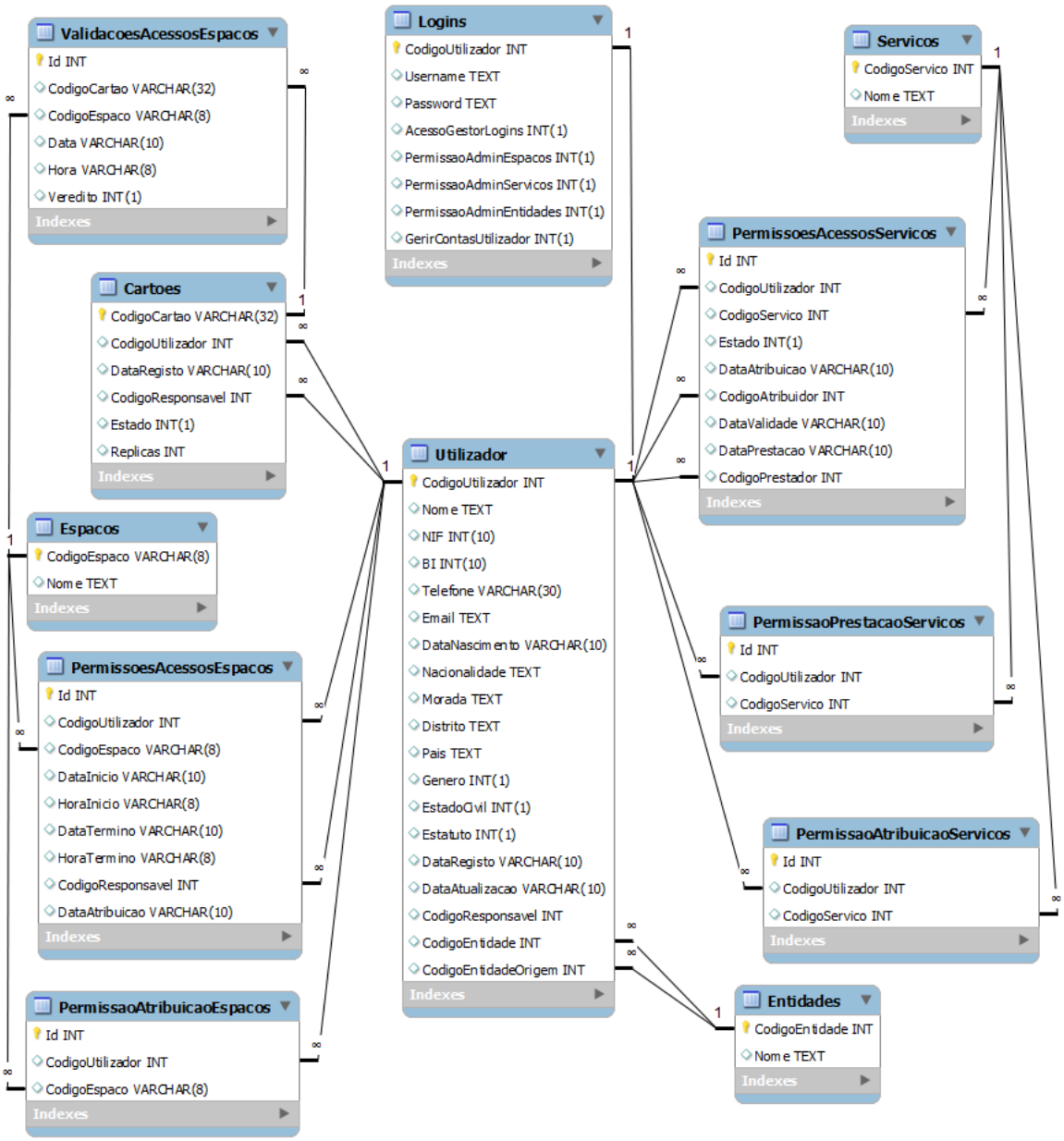


Figura 4.43: constituição e diagrama relacional UML da base de dados (f.p)

Por questões de segurança relacionadas com a captura de *passwords*, estas encontram-se armazenadas sob encriptação MD5 (62), não sendo possível o retorno para a palavra que lhe deu origem.

4.4 Servidor do Sistema

A arquitetura do sistema centralizada, logo é necessário que este integre um servidor como dispositivo responsável por atender todas as requisições efetuadas pelos clientes, ou seja, por todos os dispositivos dispersos e constituintes do sistema.

A ligação entre os clientes e o servidor é do tipo TCP/IP, sendo efetuada, através da rede internet, transmissões de mensagens HTTP. Sendo assim, o conceito de servidor que melhor ajuste apresenta com as características é um servidor web. Dada a necessidade de interpretação PHP, capacidade de alojamento e gestão de base de dados MySQL, o servidor deverá constituir-se como servidor MySQL e servidor Apache, como esquematicamente demonstra a figura 4.44.

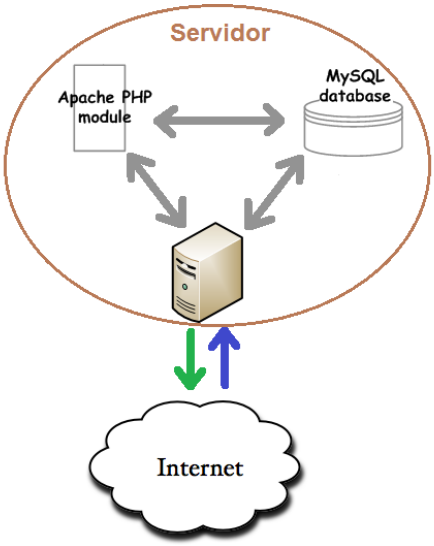


Figura 4.44: servidor do sistema (f.p)

Embora ambos (Apache e MySQL) possam integrar-se em dois dispositivos distintos, por questões de eficiência funcional, a integração num único possibilitará melhores resultados.

Conclusão

Atendendo à atual diversidade de funções desempenhadas por sistemas tecnológicos, a simplicidade e intuição de utilização e o ajuste com as necessidades são os critérios relevantes ao destaque de uma solução tecnológica. Embora os sistemas genéricos apresentem compatibilidade com uma maior diversidade de aplicações, a não especificidade poderá refletir insuficiência das respostas relativamente às atuais exigências e necessidades. Baseado nesta abordagem, o autor assumiu preferência pelo desenvolvimento de um sistema de menor abrangência quanto à compatibilidade de aplicações, contudo de maior especificidade e rigor ajustando-o às necessidades hoteleiras. O autor propõe a integração das duas funcionalidades (acessos a serviços e a espaços) num único sistema, reunindo características de distinção, potencializando o sistema. Analisando criteriosamente, ainda que o sistema seja constituído pelas duas funcionalidades, ambas definem-se como independentes podendo ser utilizadas individualmente sem que problemas funcionais ou falhas de segurança ocorram. Uma vez que o acesso à informação depende da prévia configuração dos dados que os utilizadores podem aceder, cada um somente terá acesso às funcionalidades e informações a ele autorizadas. Sendo a interface com o sistema de informação constituída por um conjunto de aplicações, a restrição de acesso às funcionalidades depende somente da não autorização de acesso às respetivas aplicações.

Relativamente à comprovação funcional do sistema, nenhum ensaio foi efetuado em cenário real, no entanto, segundo os diversos testes efetuados pelo autor em ambiente laboratorial, ainda que limitados quanto ao volume de dispositivos e à dispersão geográfica dos mesmos, demonstraram total coerência com os objetivos pretendidos. O autor destaca o reforço de ensaios efetuados na tentativa de encontrar problemas funcionais dos dispositivos, principalmente nos constituintes do sistema de validação de acessos a espaços e falhas de segurança, pela tentativa de acesso indevido à informação. Dos testes efetuados, o autor conclui que o sistema admitiu um comportamento estável não sendo denunciada qualquer falha.

Numa perspetiva de continuidade futura de desenvolvimento, o autor destaca algumas características que poderiam definir melhorias para o sistema. Relacionado com a rede de comunicação sem fios Zigbee, o autor propõe a possibilidade de integrar equipamentos como *routers* Zigbee, possibilitando outras topologias de rede, aumentando as distâncias entre dispositivos conectados a um mesmo coordenador. Esta característica permitirá também reduzir o número de módulos centrais de validação de acessos a espaços. Ainda relacionado com a rede de comunicação dos dispositivos do sistema de validação de acessos a espaços, recordando a possibilidade de utilização dos adaptadores MOD-RS-485 abordados no tópico 4.1.4.4, o autor realça a execução futura de um estudo de viabilidade sobre o desenvolvimento de *firmware,* possibilitando a compatibilidade de comunicação entre os dispositivos constituintes recorrendo a um barramento RS-485. Relacionado com a interação dos utilizadores, o autor propõe o desenvolvimento de uma interface tipo página web, possibilitando aos utilizadores, principalmente utilizadores de estatuto "Cliente", consultar dados de seu interesse tais como, permissões atribuídas tanto a espaços como a serviços e ainda prestações de serviços efetuados. O autor realça que esta característica depende praticamente do desenvolvimento da interface gráfica correspondente, uma vez que o sistema, pela sua arquitetura, reúne atualmente todas as condições e informações necessárias, não sendo necessário criar qualquer adaptação. Ainda relacionado com a interação do utilizador, o autor propõe o estudo de viabilidade na utilização da tecnologia NFC como metodologia redundante de identificação de utilizadores. Recordando a análise descrita no tópico 3.3, o autor salienta que os equipamentos de interação com as etiquetas RFID foram selecionados atendendo também as características de compatibilidade com NFC. O sistema não reúne atualmente a capacidade de identificação com recurso a NFC, uma vez que foi atribuída prioridade à tecnologia RFID por apresentar atualmente maior ajuste para o setor e o público-alvo respetivo, no entanto, o autor não despreza o potencial que a futura integração da tecnologia NFC pode amealhar para o sistema. O autor destaca que a compatibilidade funcional com esta tecnologia dependerá principalmente da adaptação do *firmware* dos dispositivos que integram equipamentos de interação para identificação, no entanto, poderão também ser necessárias redefinições no sistema de informação.

Em suma, o autor defende o adequado funcionamento do sistema, baseando-se nos ensaios funcionais, porém assume que a garantia de viabilidade de utilização deste sistema depende da prévia avaliação resultante da temporária e experimental utilização em cenário real. O autor realça as otimizações futuras enunciadas, como forma de potencializar continuamente o sistema, aumentando o ajuste com as necessidades.

Bibliografia

1. **Economia, Ministério da.** Quadros Estatísticos, Hóspedes. *Turismo de Portugal.* [Online] 14 de Agosto de 2013. [Citação: 01 de Maio de 2014.] http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/hospedes/Documents/H%C3%B3spedes%202004-2012%20Portugal_Mercados%20-%20TOP%2025.pdf.

2. —. Quadros Estatísticos, Hóspedes. *Turismo de Portugal.* [Online] 15 de Abril de 2014. [Citação: 01 de Maio de 2014.] http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/hospedes/Documents/H%C3%B3spedes%202013%20Portugal_Mercados%20-%20TOP%2010.pdf.

3. —. Quadros Estatísticos, Receitas. *Turismo de Portugal.* [Online] 22 de Abril de 2014. [Citação: 01 de Maio de 2014.] http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/receitas/Documents/Receitas%20Tur%C3%ADsticas%202013%20-%20Mercados%20-%20TOP%2010.pdf.

4. —. Quadros Estatísticos, Rceitas. *Turismo de Portugal.* [Online] 22 de Outubro de 2013. [Citação: 01 de Maio de 2014.] http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/receitas/Documents/Receitas%20Tur%C3%ADsticas%202003-2012%20Por%20Pa%C3%ADs%20de%20Origem.pdf.

5. —. Quadros Estatísticos, Hóspedes. *Turismo de Portugal.* [Online] 15 de Abril de 2014. [Citação: 01 de Maio de 2014.]

http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/hospedes/Documents/H%C3%B3spedes%202013%20Portugal_Tipologias.pdf.

6. **Cifial.** Produtos. *Cifial.* [Online] Cifial. [Citação: 15 de Maio de 2014.] http://www.cifial.pt/w4teste/door/doorn1.asp?gArea=Controlo%20de%20Acessos%20Pincode.

7. **Ponto, Guia Relógio de.** Relógio Biométrico. *Guia Relógio de Ponto.* [Online] Guia Relógio de Ponto, 2014. [Citação: 15 de Maio de 2014.] http://www.guiarelogiodeponto.com/como-funciona-o-relogio-de-ponto-biometrico.html.

8. **Incorporated, Barcoding.** Barcode Hiistory. *Barcoding.* [Online] Barcoding Incorporated, 2003. [Citação: 02 de Maio de 2014.] http://www.barcoding.com/information/barcode_history.shtml.

9. **MakeBarcode.** Types of Barcodes. *makebarcode.com.* [Online] makebarcode.com. [Citação: 02 de Maio de 2014.] http://www.makebarcode.com/specs/speclist.html.

10. **Mobile-QR-Codes.** History of QR Codes. *Mobile-QR-Codes.org.* [Online] Mobile-QR-Codes.org. [Citação: 02 de Maio de 2014.] http://www.mobile-qr-codes.org/history-of-qr-codes.html.

11. **ConsultingSolutions.** QRCode. *Consulting Solutions.* [Online] Consulting Solutions, 2014. [Citação: 02 de Maio de 2014.] http://www.ltconsulting.co.uk/why-use-a-qr-code/.

12. **L.L.C., Island Sands Computers.** Magnetic swipe cards. *Island Sands Computers L.L.C.* [Online] Island Sands Computers L.L.C., 2013. [Citação: 02 de Maio de 2014.] http://iscuae.com/products-2/magnetic-swipe-cards/.

13. **Ferreira, Daniel.** Trabalhos. *Faculdade de Engenharia da Universidade do Porto.* [Online] 06 de Dezembro de 2011. [Citação: 02 de Maio de 2014.] http://web.fe.up.pt/~jmcruz/ssi/ssi.1112/trabs-als/final/G8T8-ecard.info-final.pdf.

14. **Innoozest.** Smart Card Technology. *Innoozest.* [Online] Innoozest Technology, 2013. [Citação: 02 de Maio de 2014.] http://www.innoozest.com/smart_card_software_in_chennai.html.

15. **ComputerWorld.** Tecnologias. *ComputerWorld.* [Online] ComputerWorld Portugal, 24 de Julho de 2013. [Citação: 02 de Maio de 2013.] www.computerworld.com.pt.

16. **Notebook, Notebook - Guia do.** Leitores Biométricos. *Notebook - Guia do Notebook .* [Online] Notebook - Guia do Notebook . [Citação: 02 de Maio de 2014.] http://www.notebooks-site.com/blog/leitores-biometricos-e-possivel-falsificar-a-impressao-digital/.

17. **NControl.** Biometria. *NControl.* [Online] NControl. [Citação: 02 de Maio de 2014.] http://www.ncontrol.com.pt/component/content/article/7-faqs/66-o-que-e-a-biometria.html.

18. **Politécnica, Escola.** Biometria - Reconhecimento de Íris. *GTA Escola Politécnica.* [Online] Escola Politécnica, 03 de Junho de 2008. [Citação: 02 de Maio de 2014.] http://www.gta.ufrj.br/grad/08_1/iris/.

19. **Discovery, Google.** Google Discovery. *Google Discovery.* [Online] Google Discovery, 20 de Dezembro de 2013. [Citação: 02 de Maio de 2014.] http://googlediscovery.com/2013/12/20/samsung-vai-explorar-tecnologia-de-reconhecimento-de-iris-em-2014/.

20. **Roberti, Mark.** The History of RFID Technology. *RFID Journal.* [Online] RFID Journal LLC, 16 de Janeiro de 2005. [Citação: 05 de Maio de 2014.] http://www.rfidjournal.com/articles/view?1338.

21. **Rodrigues, Pedro João.** *Identificação por Dispositivos de Radiofrequência - RFID.* Bragança : Instituto Politécnico de Bragança, 2006. Artigo.

22. **Consultants.com, RFID.** RFID Consultants. *RFID Consultants.* [Online] RFID Consultants.com, 2012. [Citação: 05 de Maio de 2014.] http://www.rfidconsultants.com/rfid.htm.

23. **Online, Automóveis.** Automóveis Online. *Automóveis Online.* [Online] Automóveis Online. [Citação: 05 de Maio de 2014.] http://noticias.automoveis-online.com/escandalo-via-verde-pode-vir-a-ser-obrigatoria-para-todos-os-condutores/.

24. **Almeida, João Carlos.** *Novo Sistema de Rastreabilidade Industrial.* Departamento de Engenharia Mecânica, Universidade de Aveiro. Aveiro : Universidade de Aveiro, 2012. Dissertação de Mestrado.

25. **13.56MHz, RFID contactless.** RFID contactless 13.56MHz. *RFID contactless 13.56MHz.* [Online] RFID contactless 13.56MHz, 2009. [Citação: 05 de Maio de 2014.] http://srd-rfidcontactless.comoj.com/index.html.

26. **RFIDBR.** RFIDBR. *RFIDBR.* [Online] RFIDBR, 2014. [Citação: 02 de Maio de 2014.] http://www.rfidbr.com.br/index.php/tags-rfid.html.

27. **Times, NFC.** NFC Times. *Notícias.* [Online] NFC Times, 04 de Novembro de 2012. [Citação: 02 de Maio de 2014.] http://nfctimes.com/news/canadian-telco-rogers-launch-nfc-service-month-bank-blackberrys.

28. **Communication.org, Near Field.** Technology. *Near Field Communication.* [Online] Near Field Communication.org. [Citação: 02 de Maio de 2014.] http://www.nearfieldcommunication.org/technology.html.

29. **Alliance, ZigBee.** ZigBee Alliance. *ZigBee Alliance.* [Online] ZigBee Alliance. [Citação: 19 de Maio de 2014.] https://www.zigbee.org/.

30. **IEEE.** IEEE 802.15. *IEEE 802.15 Group 4.* [Online] IEEE. [Citação: 19 de Maio de 2014.] http://www.ieee802.org/15/pub/TG4.html.

31. **Janeiro, Universidade Federal do Rio de.** Redes sem fios. *Redes sem fios.* [Online] Universidade Federal do Rio de Janeiro, 06 de Junho de 2008. [Citação: 19 de Maio de 2014.] http://www.gta.ufrj.br/grad/08_1/rssf/Padres.html.

32. **Alliance, ZigBee.** Learn More. *ZigBee Alliance.* [Online] 03 de Outubro de 2003. [Citação: 19 de Maio de 2014.] https://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162.

33. —. Learn More. *ZigBee Alliance.* [Online] 11 de Agosto de 2005. [Citação: 19 de Maio de 2014.] https://docs.zigbee.org/zigbee-docs/dcn/05-3876.pdf.

34. —. Learn More. *ZigBee Alliance.* [Online] 2011. [Citação: 19 de Maio de 2014.] https://docs.zigbee.org/zigbee-docs/dcn/07-5219.PDF.

35. —. Learn More. *ZigBee Alliance.* [Online] Outubro de 2013. [Citação: 19 de Maio de 2014.] https://www.zigbee.org/portals/0/documents/whitepapers/ZigBee_WhitePaper_NextGenerationShopping_wkg2c%20%283%29%28RS%29%28Oct-7%29.pdf.

36. **Santos, José Paulo.** *Protocolo Modbus.* Departamento de Engenharia Mecânica. Aveiro : Universidade de Aveiro, 2010.

37. **Organization, Modbus.** Technical Resources. *Modbus.* [Online] 26 de Abril de 2012. [Citação: 21 de Maio de 2014.] http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.

38. —. Technical Resources. *Modbus.* [Online] Junho de 1996. [Citação: 21 de Maio de 2014.] http://www.modbus.org/docs/PI_MBUS_300.pdf.

39. **Moreira, Pedro.** *Gestão e controlo de acessos.* Departamento de Engenharia Eletrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto. Porto : Universidade do Porto, 2008. Dissertação de Mestrado.

40. **Teixeira, Manuel.** *Projecto de implementação RFID na empresa ATEC.* Departamento de Engenharia Eletrotécnica, Instituto Superior de Engenharia do Porto. Porto : Instituto Superior de Engenharia do Porto, 2008. Dissertação de Mestrado.

41. **Telemax.** Produtos. *Telemax.* [Online] [Citação: 01 de Maio de 2014.] http://www.telemax.pt/catalogo.aspx?idcat=44.

42. **Sursystems.** Fechaduras de Hotel RFID. *Sursystems.* [Online] Sursystems. [Citação: 01 de Maio de 2014.] http://www.sursystems.pt/Promo%C3%A7%C3%B5es/FechadurasdeHotelRFID.aspx.

43. **cifial.** Catálogos de Produtos. *Cifial.* [Online] [Citação: 01 de Maio de 2014.] http://www.cifial.pt/w4teste/door/pdfs/hca.pdf.

44. **Janeiro, Universidade Federal do Rio de.** O que são redes P2P. *Poluição em redes P2P.* [Online] Universidade Federal do Rio de Janeiro, 16 de Outubro de 2008. [Citação: 22 de Abril de 2014.] http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/renan_bernardo/p2p.html.

45. **Steve Mackay, Steve Mackay, DeonReynders, John Park.** *Practical Industrial Data Networks: Design,.* s.l. : ELSEVIER, 2004.

46. **Sparkfun.** RFID Evaluation Shield - 13.56MHz. *Sparkfun.* [Online] Sparkfun Eletronics. [Citação: 17 de Fevereiro de 2014.] https://www.sparkfun.com/products/10406.

47. —. SM130 datasheet. *Sparkfun.* [Online] Março de 2008. [Citação: 17 de Fevereiro de 2014.] https://www.sparkfun.com/datasheets/Sensors/ID/SM130.pdf.

48. **Adafruit.** PN532 NFC/RFID controller breakout board. *Adafruit.* [Online] Adafruit. [Citação: 03 de Março de 2014.] https://www.adafruit.com/products/364.

49. **Semiconductors, NXP.** PN532 User Manual. *Adafruit.* [Online] 05 de Novembro de 2007. [Citação: 03 de Fevereiro de 2014.] http://www.adafruit.com/datasheets/pn532um.pdf.

50. **Microchip.** MCP2200 datasheet. *Microchip.* [Online] 03 de 10 de 2011. [Citação: 15 de Maio de 2014.] http://ww1.microchip.com/downloads/en/DeviceDoc/22228B.pdf.

51. —. PIC18F2420/2520/4420/4520 datasheet. *Microchip.* [Online] Microchip, 21 de Novembro de 2008. [Citação: 11 de Fevereiro de 2014.] http://ww1.microchip.com/downloads/en/DeviceDoc/39631E.pdf.

52. **Digi.** XBee ZB. *Digi.* [Online] Digi. [Citação: 03 de Fevereiro de 2014.] http://www.digi.com/products/wireless-wired-embedded-solutions/zigbee-rf-modules/zigbee-mesh-module/xbee-zb-module#overview.

53. **Olimex.** MOD-ZIGBEE-UEXT . *Olimex.* [Online] Olimex. [Citação: 04 de Novembro de 2013.] https://www.olimex.com/Products/Modules/RF/MOD-ZIGBEE-UEXT/.

54. **Microchip.** PIC18F23K20/24K20/25K20/26K20/43K20/44K20/45K20/46K20 datasheet. *Microchip.* [Online] 04 de Setembro de 2010. [Citação: 04 de Novembro de 2013.] http://ww1.microchip.com/downloads/en/DeviceDoc/41303G.pdf.

55. —. MRF24J40 datasheet. *Microchip.* [Online] 08 de Agosto de 2010. [Citação: 04 de Novembro de 2013.] http://ww1.microchip.com/downloads/en/DeviceDoc/39776C.pdf.

56. **Olimex.** Project Demo Zigbee. *Olimex.* [Online] 31 de Maio de 2011. [Citação: 04 de Novembro de 2013.] https://www.olimex.com/Products/Modules/RF/MOD-ZIGBEE-UEXT/resources/MOD-ZIGBEE_PowerPoint.zip.

57. **Microchip.** PIC32MX1XX/2XX datasheet. *Microchip.* [Online] 03 de Março de 2014. [Citação: 14 de Abril de 2014.] http://ww1.microchip.com/downloads/en/DeviceDoc/60001168F.pdf.

58. **Aliexpress.** Serial WiFi Ethernet (dual RJ45) rs232/rs485 WiFi module. *Aliexpress.* [Online] Aliexpress. [Citação: 02 de Abril de 2014.] http://www.aliexpress.com/item/WIFI-to-rs232-module-Start-Kit-free-shipping/1286647017.html.

59. **Olimex.** MOD-RS485 datasheet. *Olimex.* [Online] Abril de 2011. [Citação: 20 de Janeiro de 2014.] https://www.olimex.com/Products/Modules/Interface/MOD-RS485/resources/MOD-RS485.pdf.

60. **Poupa, Alexandre Pereira e Carlos.** *Linguagens WEB.* [ed.] Manuel Robalo. Lisboa : Edições Silabo, 2004. Vol. 1ªEdição.

61. **Microsoft.** *Microsoft Visual Basic.Net Passo a Passo.* Portugal : McGraw-Hill, 2002.

62. **Corporation, EMC.** RSA Laboratories. *EMC2.* [Online] EMC Corporation. [Citação: 12 de Maio de 2014.] http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/md2-md4-and-md5.htm.

63. **mysqlconnector.** Downloads. *MySQL.* [Online] [Citação: 10 de Maio de 2014.] http://dev.mysql.com/get/Downloads/Connector-Net/mysql-connector-net-1.0.10.exe.

64. **Damas, Luís.** *SQL-Structured Query Language - 6ªEdição Actualizada e Aumentada.* s.l. : FCA.

65. **Semiconductors, NXP.** Mifare Classic 1K datasheet. *NXP Semiconductors.* [Online] 21 de Fevereiro de 2011. [Citação: 10 de Maio de 2014.] http://www.nxp.com/documents/data_sheet/MF1S503x.pdf.

66. **Wikipedia.** UEXT. *Wikipedia.* [Online] Wikipedia. [Citação: 02 de Dezembro de 2013.] http://en.wikipedia.org/wiki/UEXT.

67. **Integrated, Maxim.** MAX3222-MAX3241 datasheet. *Maxim Integrated.* [Online] Janeiro de 2007. [Citação: 02 de Abril de 2014.] http://datasheets.maximintegrated.com/en/ds/MAX3222-MAX3241.pdf.

68. **Instruments, Texas.** LM1117 datasheet. *Texas Instruments.* [Online] Março de 2013. [Citação: 25 de Abril de 2014.] http://www.ti.com/lit/ds/symlink/lm1117-n.pdf.

69. —. LM7805 datasheet. *Texas Instruments.* [Online] Agosto de 2012. [Citação: 01 de Abril de 2014.] http://www.ti.com/lit/ds/symlink/ua7805.pdf.

70. **Philips.** PN532 datasheet. *Adafruit.* [Online] 31 de Março de 2011. [Citação: 03 de Fevereiro de 2014.] http://www.adafruit.com/datasheets/pn532ds.pdf.

71. **Instruments, Texas.** LM3940 datasheet. *Texas Instruments.* [Online] Março de 2013. [Citação: 01 de Abril de 2014.] http://www.ti.com.cn/cn/lit/ds/symlink/lm3940.pdf.

Anexos

A1 – Mensagens de leitura e escrita de etiquetas RFID.

A figura A1.1 apresenta um diagrama de interação entre os equipamentos exemplificando a leitura e escrita numa etiqueta RFID tipo Mifare.

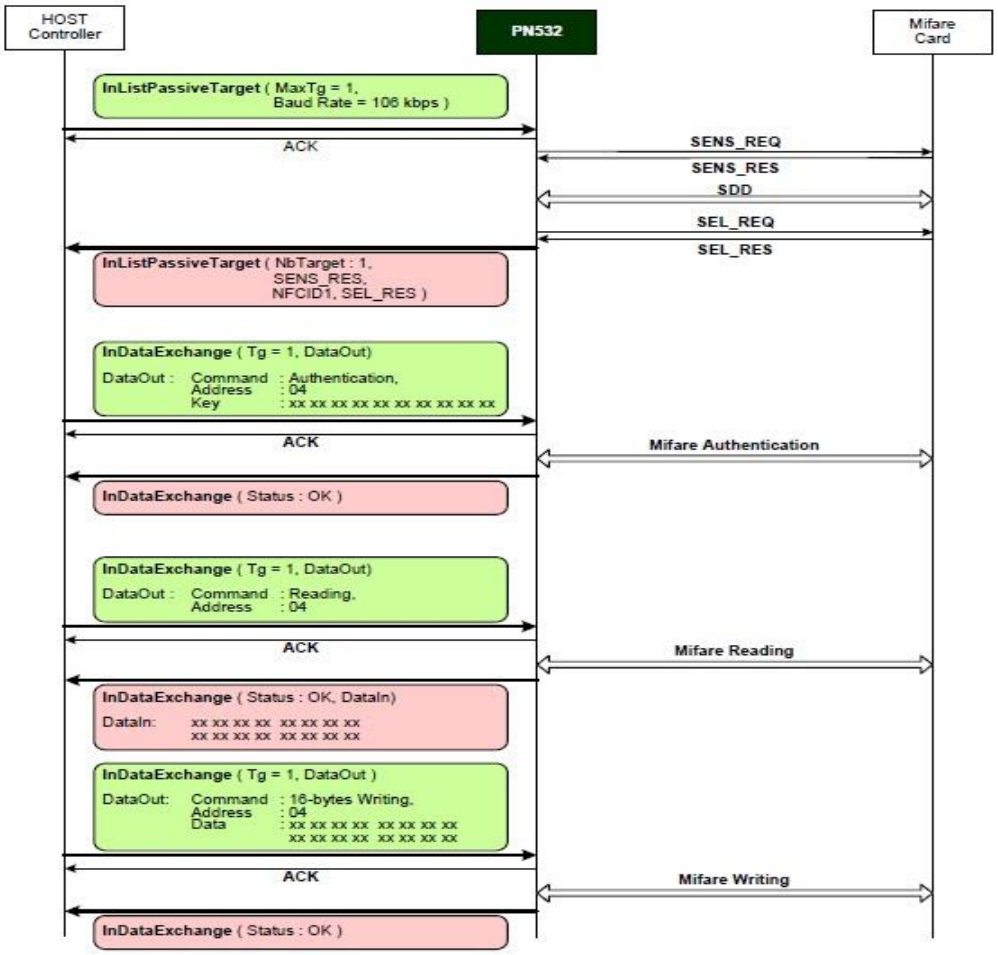


Figura A1.1: interação para escrita e leitura de etiquetas RFID Mifare (49)

A2 – Metodologias de comunicação I2C

A figura A2.1 apresenta dois diagramas de comunicação I2C entre os equipamentos. O primeiro representa a metodologia de comunicação sem recurso ao sinal digital de sincronismo entre equipamentos, sendo o segundo referente à metodologia contrária.

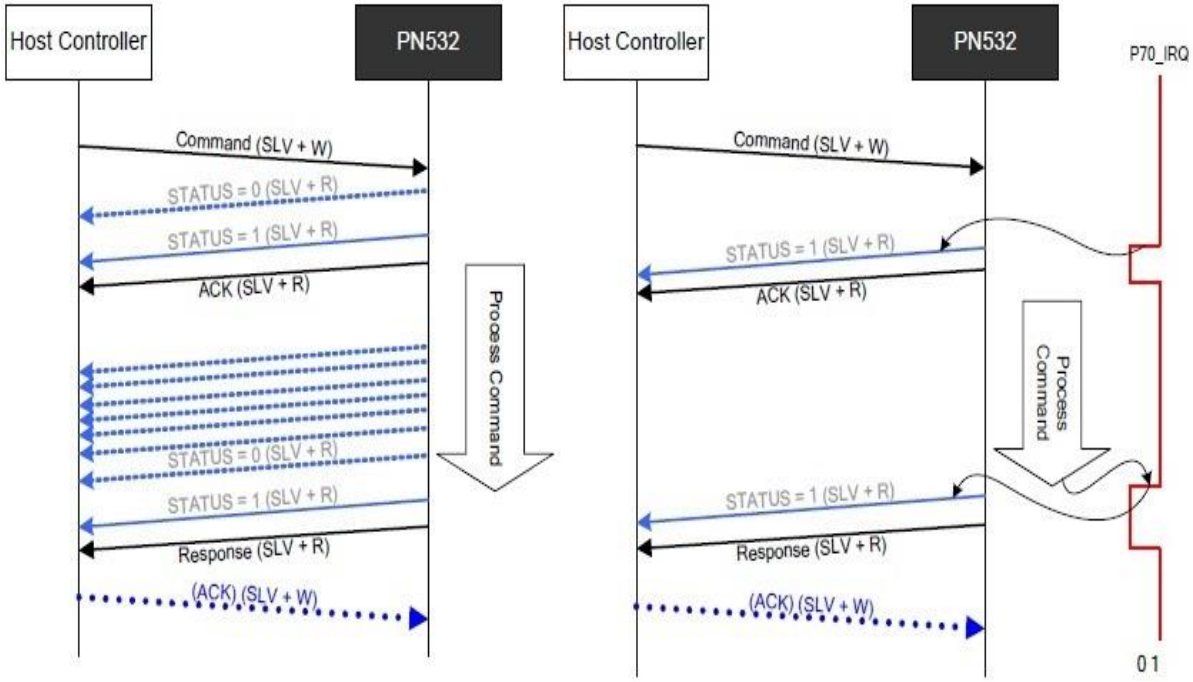


Figura A2.1: diagramas de comunicação I2C referentes às duas metodologias (49)

A3 – Memória de dados de etiquetas RFID Mifare

A figura A3.1 apresenta esquematicamente a organização da memória de dados (EEPROM) integrada em etiquetas RFID tipo Mifare.

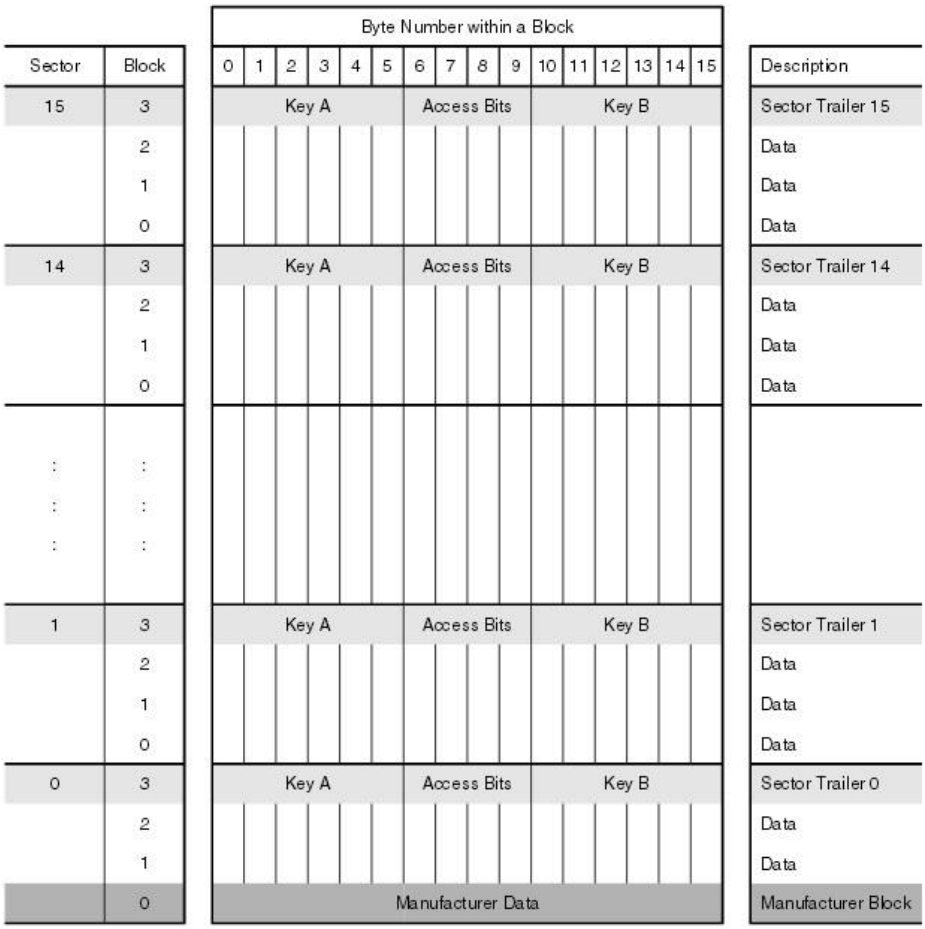


Figura A3.1: organização da memória de dados de etiquetas RFID Mifare (65)

A4 – Dispositivo de leitura e escrita de etiquetas RFID

A Figura A4.1 representa esquematicamente o circuito elétrico do dispositivo de leitura e escrita de etiquetas RFID.

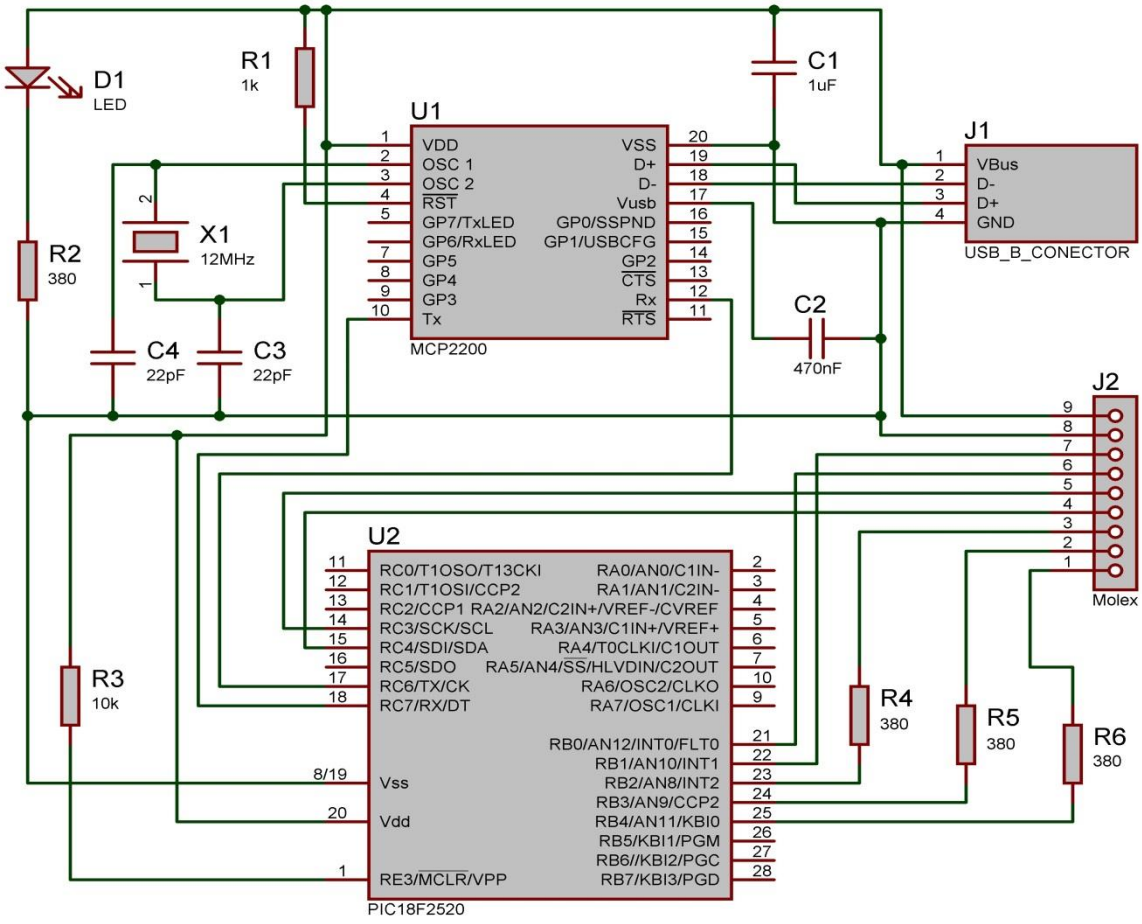


Figura A4.1: esquema elétrico do dispositivo de leitura e escrita de etiquetas RFID (f.p)

A5 - Dispositivo de identificação para acesso a espaços

A figura A5.1 representa o esquema elétrico do dispositivo de identificação para acesso a espaços.

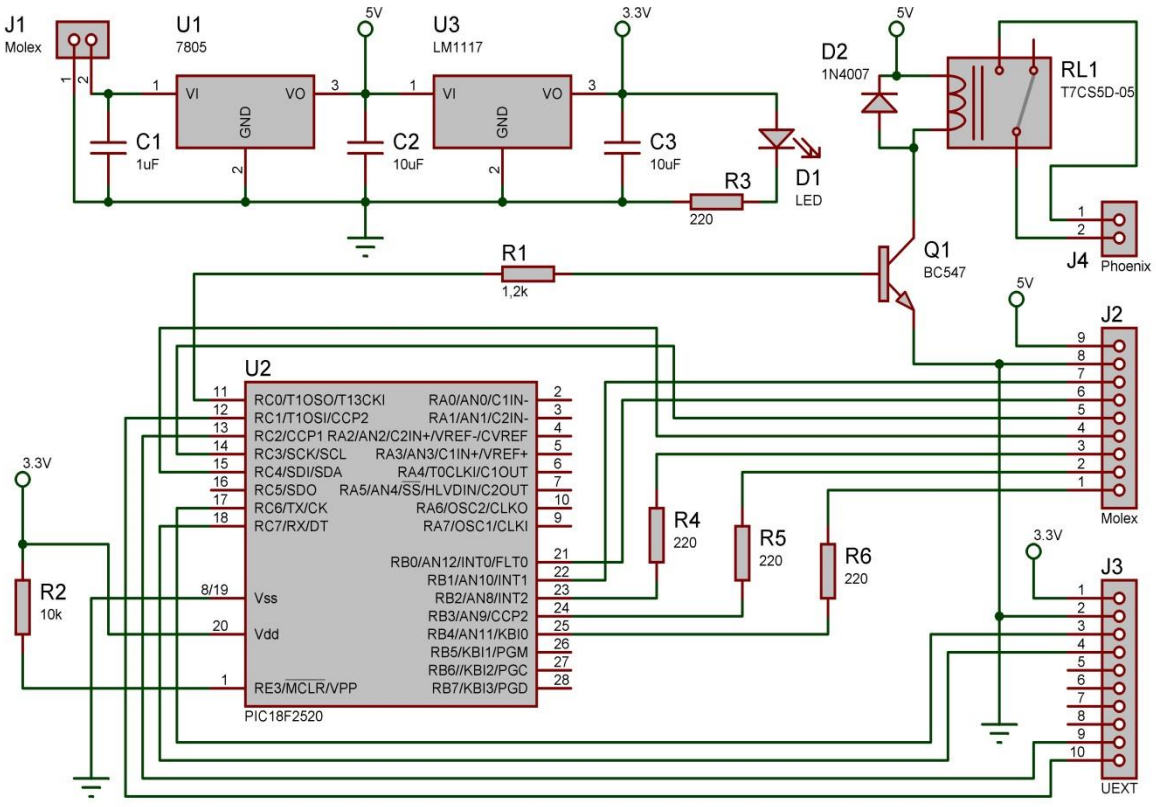


Figura A5.1: esquema elétrico do dispositivo de identificação para acesso a espaços (f.p)

A6 - Módulo central de validação de acesso a espaços

A figura A6.1 representa o esquema elétrico do módulo central de validação de acesso a espaços.

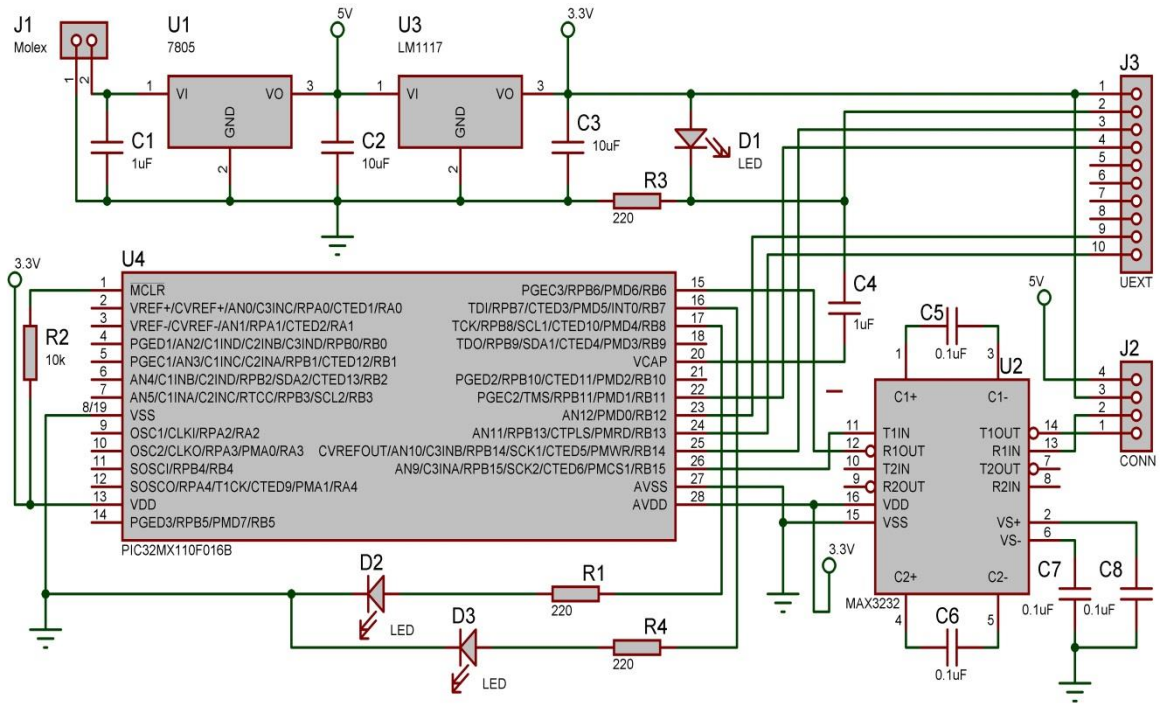


Figura A6.1: esquema elétrico módulo central de validação de acesso a espaços (f.p)

A7 – Rede de comunicação Zigbee

O trabalho descrito neste anexo foi desenvolvido com o propósito de possibilitar uma melhor consolidação dos conhecimentos referentes à tecnologia de comunicação sem fios Zigbee, através da programação de microcontroladores necessária para configurações funcionais específicas. Os equipamentos utilizados no trabalho foram os MOD-ZIGBEE-UEXT da Olimex (53) e a implementação dos algoritmos referentes à comunicação Zigbee foi efetuada, recorrendo à *stack* Zigbee da Microchip (56) disponibilizada pelo fabricante dos Equipamentos.

Objetivo

O trabalho propõe a configuração dos equipamentos selecionados para que possibilitem duas abordagens funcionais:

- Transmissão transparente;
- Controlo e aquisição;

Ambas as funcionalidades requerem a capacidade de diálogo entre os respetivos equipamentos. Dado a intenção do trabalho, a comunicação entre os equipamentos será Zigbee.

Funcionalidade transmissão transparente

Esta funcionalidade prevê possibilitar a troca de mensagens entre dispositivos com recurso aos equipamentos configurados. O objetivo desta funcionalidade é possibilitar a integração de meios de comunicação sem fios a sistemas constituídos por dispositivos que

somente apresentam interfaces de comunicação cablada (Ex: UART). Um cenário exemplo para a integração do sistema é representado na figura A7.1.

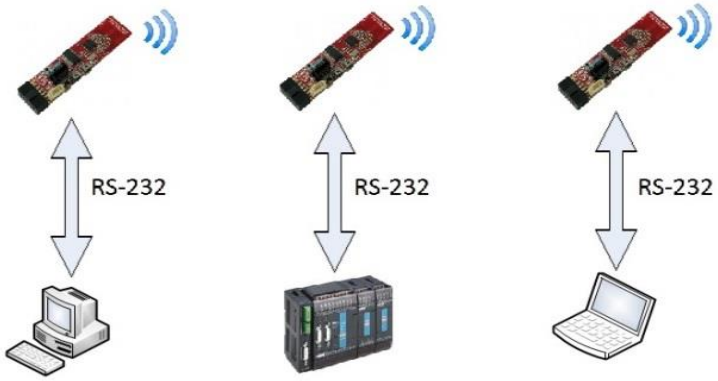


Figura A7.1: sistema exemplo que recorre a equipamentos de comunicação sem fios (f.p)

Funcionalidade controlo e aquisição

Esta funcionalidade pretende possibilitar o controlo e aquisição de estados de interfaces de equipamentos remotamente, ou seja, monitorizar saídas digitais, entradas digitais e entradas analógicas e controlar saídas digitais, através de mensagens protocoladas. O objetivo desta funcionalidade é potencializar os equipamentos de comunicação sem fios com a integração de funções paralelas relevantes a sistemas que os possam integrar. A Figura A7.2 apresenta um sistema exemplo que implementa os equipamentos pela necessidade de aquisição e controlo remoto.

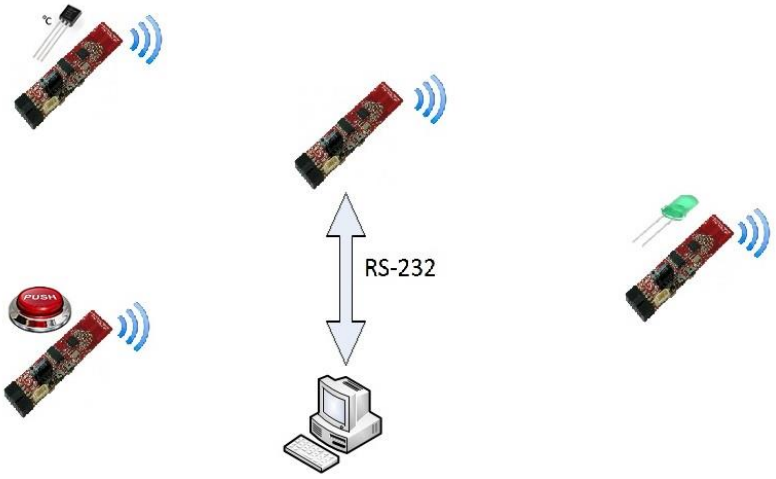


Figura A7.2: sistema exemplo de Controlo e aquisição (f.p)

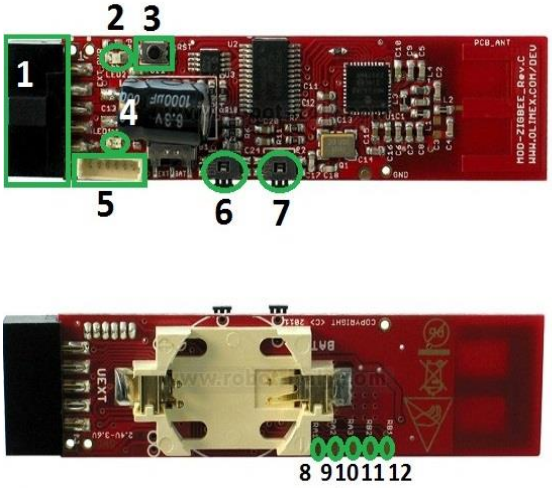
Equipamento

Como anteriormente descrito, os equipamentos utilizados no desenvolvimento deste trabalho são os MOD-ZIGBEE-UEXT da Olimex (53) (Figura A7.3).

Figura A7.3: MOD-ZIGBEE-UEXT (53)

Estes equipamentos são constituídos por um microcontrolador (PIC18F26k20) (54) e um *transceiver* RF (MRF24J40) (55). Encontrando-se acessíveis as interfaces de comunicação necessárias à programação do microcontrolador, é possível configurar o funcionamento dos equipamentos. Uma vez que o *transceiver* respeita todas as características físicas da tecnologia Zigbee, estes equipamentos podem ser configurados de forma a comunicarem com recurso a esta tecnologia de comunicação.

Para além das características enunciadas, os equipamentos possibilitam a interação através do acesso a diversas interfaces do microcontrolador. A Figura A7.4 demonstra e descreve a constituição das interfaces dos equipamentos.



Legenda

1 - Ficha UEXT
2 - Led Verde (RA1)
3 - Botão Reset (MCLR)
4 - Led Vermelho (RA0)
5 - Ficha Mini ICSP
6 - Botão de pressão 2 (RB4)
7 - Botão de pressão 1 (RB5)
8 - Digital Input/output (RA7)
9 - Digital Input/output (RA6)
10 - Digital Input/output (RA4)
11 - Digital Input/output (RB3) & input analógico (AN9)
12 - Digital Input/output (RB2) & input analógico (AN8)

Figura A7.4: interfaces disponíveis no equipamento (53)(adaptada)

Não sendo na Figura A7.4 percetíveis as conexões disponíveis no conector UEXT, a Figura A7.5 descreve-as pormenorizadamente.

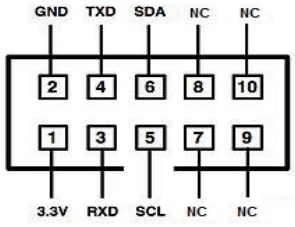


Figura A7.5: conexão ficha UEXT (66)(adaptada)

Configuração e programação

Com o intuito de possibilitar a compreensão do processo de programação, serão descritos os procedimentos necessários para configurar os equipamentos de modo a que possam ser conectados a dois computadores, possibilitando o envio de um caracter entre eles. A figura A7.6 esquematiza o funcionamento previsto.

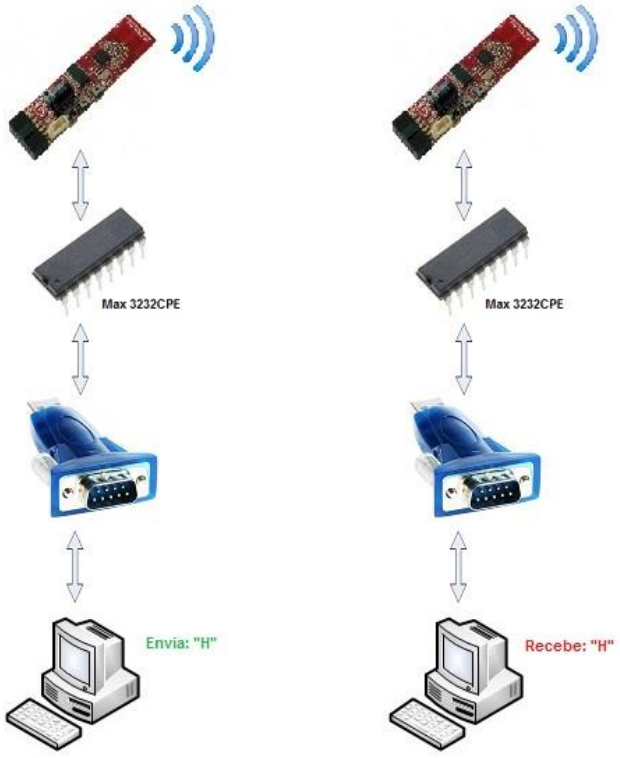


Figura A7.6: envio de carater entre dois computadores (f.p)

Para a montagem e posterior funcionamento do sistema é necessário atender os seguintes requisitos:

1. Hardware:
   - 2 Adaptadores USB-to-RS-232;
   - 2 MAX 3232 CPE (67) ou semelhante;
   - 2 equipamentos MOD-ZIGBEE-UEXT;
   - 2 Circuitos reguladores (3,3V);

2. Firmware:
   - *Stack* ZigBee Microchip;

3. Software:
   - MPLAB IDE;
   - Compilador C18 da Microchip;
   - Hyperterminal ou semelhante;

Após estarem garantidos todos os requisitos enunciados, deverá ser efetuada a programação dos dispositivos de acordo com o objetivo pretendido. No processo de programação dos microcontroladores dos equipamentos, deverão ser atendidas as seguintes definições:

- Parâmetros da comunicação serie UART (*defeito*: 19200,8,N,1);
- Endereço do equipamento Zigbee;
- Canal de comunicação;
- PAN ID;
- Potência do sinal RF;

As definições descritas devem ser efetuadas no ficheiro “zigbee.def”, incorporado no projeto referente à *stack* para o dispositivo pretendido.

Para este exemplo concreto, um dispositivo deverá ser configurado como Coordenador e o outro como um Dispositivo terminal. Assumindo que o coordenador estará conectado ao computador que irá receber o caracter e o dispositivo terminal estará conectado ao computador que irá enviar o caracter, a programação deverá seguir os seguintes passos:

Dispositivo terminal (emissor)

Aceder ao ficheiro "RFD.c" e declarar e inserir a função "ProcessUART" como demonstra a Figura A7.7.

```
void ProcessUART(void) {

    carater = 0;

    carater = ConsoleGet();

}
```

Figura A7.7: função ProcessUART (f.p)

De acordo com o código representado na Figura A7.7, a variável "caracter" deverá ser declarada como variável global e poderá ser do tipo BYTE ou unsigned char. A função "ConsoleGet" é uma função já definida no ficheiro "Console.c".

Como demonstra a Figura A7.8, a função "ProcessUART" deverá ser chamada na função "ProcessNONZigBeeTasks".

```
void ProcessNONZigBeeTasks(void) {
    if (ConsoleIsGetReady())
        ProcessUART();
```

Figura A7.8: código responsável pela execução da função ProcessUART (f.p)

Após Inserir o código corretamente, é necessário inserir um outro código dentro da respetiva condição de modo a possibilitar o envio da mensagem por RF (Zigbee) para o coordenador (ver Figura A7.9).

```
        case NO_PRIMITIVE:

            if (ZigBeeStatus.flags.bits.bNetworkJoined){
                    if (carater!=0){

                        ZigBeeBlockTx();
                        TxBuffer[TxData++] = carater;

                        params.APSDE_DATA_request.DstAddrMode = APS_ADDRESS_GROUP;

                        params.APSDE_DATA_request.DstAddress.ShortAddr.v[1] = 0x00;
                        params.APSDE_DATA_request.DstAddress.ShortAddr.v[0] = GROUP_ID4;

                        params.APSDE_DATA_request.SrcEndpoint = GROUP_ID4;

                        params.APSDE_DATA_request.RadiusCounter = DEFAULT_RADIUS;
                        params.APSDE_DATA_request.DiscoverRoute = ROUTE_DISCOVERY_SUPPRESS;
    #ifdef I_SUPPORT_SECURITY
                        params.APSDE_DATA_request.TxOptions.Val = 1;
    #else
                        params.APSDE_DATA_request.TxOptions.Val = 0;
    #endif

                        params.APSDE_DATA_request.TxOptions.bits.acknowledged = 0;
                        params.APSDE_DATA_request.ProfileId.Val = 0x7f01;
                        params.APSDE_DATA_request.ClusterId.Val = BUFFER_TEST_REQUEST_CLUSTER;
                        currentPrimitive = APSDE_DATA_request;

                    }
            }
```

Figura A7.9: código para envio de um caracter para o dispositivo coordenador (f.p)

Dispositivo Coordenador (recetor)

Aceder ao ficheiro “Coordinator.c” e inserir o código necessário para a receção e envio do caracter para a UART (ver Figura A7.10).

```
case BUFFER_TEST_REQUEST_CLUSTER:
{
    BYTE SeqLen = APLGet();

    ConsolePut(SeqLen);
}
break;
```

Figura A7.10: exemplo de leitura do buffer de receção e envio para a UART (f.p)

Efetuando todo este procedimento algoritmo e programando cada um dos equipamentos corretamente, após inicialização da rede Zigbee (Coordenador) e conexão do dispositivo terminal

à mesma, verificando-se a correta conexão com os computadores, poderá ser enviado um caracter de um computador para o outro.

Sistema desenvolvido

Como enunciado nos objetivos deste trabalho, pretende-se a comunicação sem fios entre vários equipamentos dispersos num espaço, através dos quais, possam ser executadas duas funcionalidades distintas: transmissão transparente e controlo e aquisição.

O sistema foi desenvolvido atendendo às imposições e, para além destas, foram concebidos algoritmos com o intuito de melhorar o comportamento de cada equipamento na rede, otimizando o comportamento global desta. Assim serão apresentados inicialmente os processos referentes a otimizações da rede, sendo posteriormente demonstrado o funcionamento do sistema desenvolvido para os dois modos descritos.

Algoritmos de correção de erros na rede (otimizações)

Os algoritmos de correção de erros da rede foram concebidos com a intenção de corrigir problemas como perda de ligação e incapacidade de estabelecer novamente conexão por parte dos equipamentos, assim como incapacidade de perceção de equipamentos ativos e inativos na rede Zigbee. A *stack* da tecnologia Zigbee utilizada como base ao desenvolvimento do sistema não prevê a identificação dos problemas e erros descritos.

Dado que o processo de demonstração funcional de todas as otimizações implementadas é complexo, somente serão descritas as situações que o sistema consegue identificar e corrigir em funcionamento continuo. Os algoritmos de correção podem ser divididos em dois grupos: coordenação dos dispositivos e atuação em caso de erro detetado.

1. Mecanismos de Coordenação dos dispositivos:
    - Um dispositivo terminal, quando inicia, verifica a existência de rede. Caso não se verifique a existência, o dispositivo terminal entra em estado inativo, reiniciando ao fim de aproximadamente 15s;
    - Quando uma rede está formada e um dispositivo terminal inicia o processo de conexão, o coordenador deteta-o e informa os restantes por forma a silencia-

los possibilitando, uma mais rápida conexão do dispositivo e com redução de probabilidade de erros de conexão.

2. Deteção de erros:
    - Se o dispositivo coordenador formou a rede mas ao fim de aproximadamente 30s não verificar nenhum dispositivo conectado (a rede poderá ter sido formada com erro e caso haja algum dispositivo terminal, este poderá não conseguir efetuar conexão) a rede é terminada e o coordenador reinicia, formando deste modo a rede novamente.
    - Se um dispositivo terminal tentar estabelecer ligação a uma rede formada e, aproximadamente após um minuto não tiver conseguido obter sucesso na conexão, será reiniciado e iniciará o processo.
    - Se um dispositivo terminal perder conexão com a rede por qualquer erro, será reiniciado após 15s e voltará a estabelecer conexão.
    - Se por motivo de erro, um dispositivo terminal conectado à rede não conseguir efetuar troca de informação corretamente com o coordenador e este detete latência na rede sem razão aparente, a rede será novamente formada, ou seja, o coordenador reiniciará e restabelecerá a rede (situação limite e somente executada em caso de impossibilidade de deteção de problema por parte do dispositivo terminal e consecutivas tentativas de alerta pelo coordenador falhadas).
    - Durante o período de rede formada, o coordenador questiona periodicamente todos os dispositivos por forma a conseguir manter a informação dos módulos conectados à rede. A inexistência deste mecanismo não colocaria em risco o funcionamento da rede, porém poderia contribuir para a latência da rede pela tentativa de sucessivas entregas de mensagens a um destinatário não conectado nesse momento e que o esteve outrora.

Funcionamento do sistema desenvolvido

Com o intuito de demonstrar as potencialidades do sistema, será ilustrado e explicado o funcionamento do sistema desenvolvido.

A demostração será efetuada em três subtópicos, sendo primeiramente explicado o sistema de sinalização do estado dos dispositivos (*leds*), juntamente com o sistema de teste de conexão dos mesmos. Subsequentemente serão apresentados os dois subtópicos restantes referentes às duas funcionalidades configuradas: transmissão transparente e controlo e aquisição.

A topologia da rede Zigbee do sistema será garantidamente estrela, uma vez que não foram incorporados equipamentos configurados como *routers.*

Sistema de sinalização

Dado que a perceção do estado funcional dos dispositivos deve ser o mais intuitiva possível, no desenvolvimento deste sistema integrou-se algoritmos capazes de, através dos Leds integrados nos equipamentos, possibilitar a aquisição do estado dos mesmos pelo utilizador. A sinalização é distinta para os dois tipos de equipamentos configurados, ou seja, dispositivos terminais e coordenador. Sendo duas configurações distintas, através de diferentes sinalizações, o utilizador facilmente poderá distinguir os equipamentos. Primeiramente será explicado o sistema de sinalização desenvolvido para os equipamentos do tipo coordenador, sendo por fim explicada a sinalização referente a dispositivos terminais.

Dispositivo Coordenador

1. Sinalizadores:
    - *Led* verde: indicador de rede;
    - *Led* vermelho: indicador de Inicialização e de mensagens transmitidas;

2. Sinalizações:
    - *Led* vermelho ON: power ON e módulo em tentativa de inicialização de rede;
    - *Led* verde intermitente (lento): rede estabelecida, modo de difusão *broadcast*;
    - *Led* verde intermitente (rápido): rede estabelecida, modo de difusão *unicast*;
    - *Led* verde intermitente e *led* Vermelho *ON* uma fração de segundo: mensagem recebida ou enviada;
    - Intermitência dos dois *leds*: dispositivo em reinicialização;

Dispositivo Terminal

1. Sinalizadores:
    - *Led* verde: indicador de inicialização e de mensagens transmitidas;
    - *Led* vermelho: indicador de conexão;

2. Sinalizações:

- *Led* verde *ON*: *power ON* e módulo em procura/tentativa de conexão à rede;
- *Led* vermelho ON: rede encontrada e conexão pré estabelecida (transmissão de dados bloqueada);
- *Led* vermelho intermitente: dispositivo conectado à rede e em normal funcionamento (transmissão de dados ativa);
- *Led* vermelho intermitente e *led* verde *ON* uma fração de segundo: mensagem recebida ou enviada;
- Intermitência dos dois leds simultaneamente: dispositivo em reinicialização;

Funcionalidade de transmissão transparente

Neste modo de funcionamento, o sistema possibilita transmissão de mensagens entre dispositivos conectados aos equipamentos através das interfaces de comunicação UART de cada um deles.

Para ativar este modo funcional, a mensagem a enviar deverá ser iniciada pelo caracter "#". Uma vez que pode ser necessário enviar mensagens para todos os dispositivos terminais simultaneamente, o coordenador admite dois modos de difusão: *broadcast* e *unicast*. A alteração entre os dois modos de difusão é efetuada através do botão de pressão 1 deste equipamento. Quando o botão 1 é premido é enviado para a UART deste equipamento uma mensagem que identifica o modo de difusão atualmente ativo. A sinalização também é feita pelo *led* verde indicador de rede formada, que aumenta a velocidade de intermitência quando em modo *unicast*.

Dependendo do modo de difusão, a estrutura das mensagens a enviar pelo dispositivo coordenador varia. As Figuras A7.11 e A7.12 representam esquematicamente a estrutura das mensagens no modo *brodcast* e no modo *unicast* respetivamente.

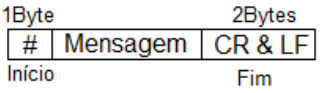


Figura A7.11: estrutura da mensagem em modo *broadcast* (f.p)

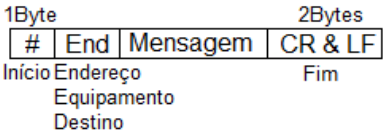


Figura A7.12: estrutura da mensagem em modo *unicast* (f.p)

A situação descrita é refente às mensagens a enviar através do equipamento configurado como coordenador. Para o caso dos dispositivos terminais, a estrutura de mensagens é única e deve respeitar uma estrutura semelhante à estrutura das mensagens a enviar, através do equipamento configurado como coordenador em modo *broadcast*. Não é necessário endereçar o destinatário pelo que a mensagem será sempre remetida ao coordenador da rede.

De modo a demonstrar funcionalmente o sistema, a Figura A7.13 demonstra a troca de mensagens entre dois computadores, dotados de programas terminais e devidamente conectados a dois equipamentos configurados como coordenador e dispositivo terminal com o endereço 0x02 e em modo *broadcast*.

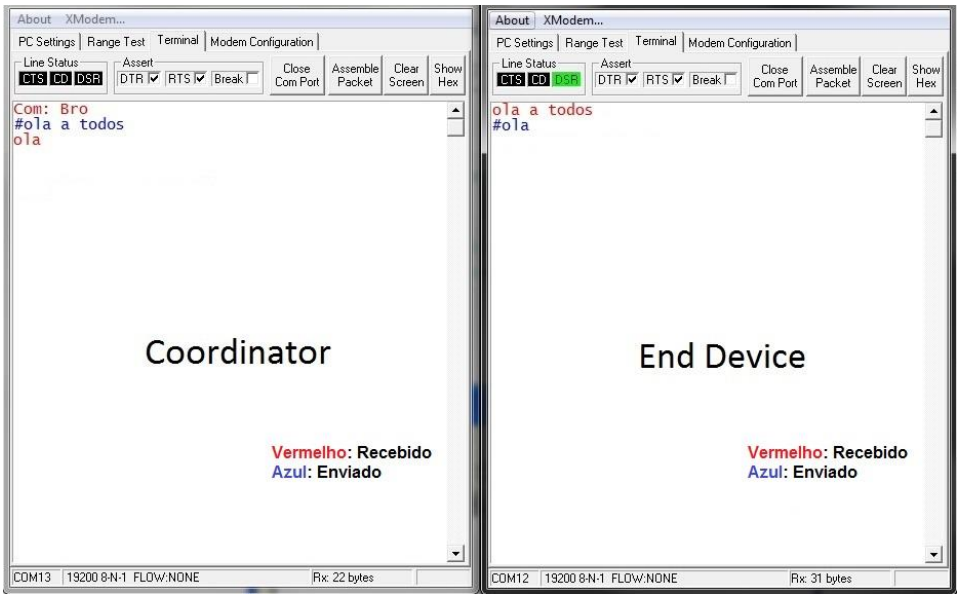


Figura A7.13: exemplo de funcionamento em modo *broadcast* (f.p)

Como é possível observar na Figura A7.13, previamente ao envio da mensagem, o modo foi alterado para *Brodcast* sendo indicado no programa terminal do computador conectado ao equipamento configurado como coordenador Zigbee. Embora não sendo percetível, a mensagem enviada pelo coordenador seria recebida por todos os dispositivos terminais conectados à rede Zigbee. A Figura A7.14 demonstra novamente a troca de mensagens entre os dois computadores porém, o coordenador encontra-se em modo de difusão *unicast*.

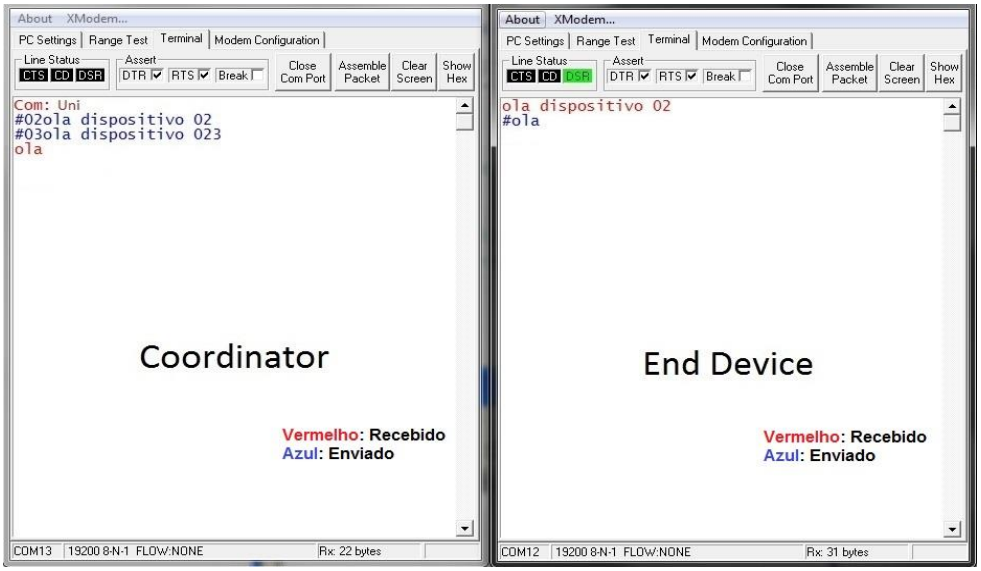


Figura A7.14: exemplo de funcionamento em modo *unicast* (f.p)

Como é possível observar, as mensagens enviadas através do coordenador são endereçadas com o destinatário. Uma vez que o endereço dispositivo terminal conectado ao segundo computador é 0x02, somente este recebe a mensagem. A segunda mensagem, enviada através do equipamento configurado como coordenador, tem como destinatário o equipamento com o endereço 0x03, pelo que não é observada no computador conectado ao dispositivo terminal endereçado 0x02.

Ainda relativamente às duas comunicações exemplo apresentadas, como é possível verificar, independentemente do modo de difusão do coordenador, o computador conectado ao equipamento configurado como dispositivo terminal envia mensagens para o coordenador não sendo necessário qualquer informação de endereço.

Funcionalidade de controlo e aquisição

Neste tópico será demonstrado o funcionamento do sistema em modo de controlo e aquisição. Esta funcionalidade recorre diretamente às interfaces: entradas e saídas digitais e entradas analógicas, disponíveis e ativas nos próprios equipamentos configurados como dispositivos terminais.

Para esta funcionalidade somente são aceites envio de mensagens através do equipamento configurado como coordenador. A estrutura das mensagens e o próprio funcionamento foram desenvolvidos com base na estrutura das mensagens definidas pelo protocolo Modbus.

Cada dispositivo terminal foi configurado de modo a possibilitar a monitorização de duas entradas digitais, duas saídas digitais e uma entrada analógica e controlar duas saídas digitais.

Dado que a requisição, ou alteração do estado de um interface, deve ser efetuada somente a um dispositivo de cada vez, o modo de difusão desta funcionalidade é *unicast*. Comparativamente ao tipo de diálogo definido pelo protocolo Modbus (*Master/Slave*), o equipamento configurado como coordenador é considerado o *Master* do sistema, sendo os dispositivos terminais os *Slaves*.

A Figura A7.15 esquematiza a estrutura das mensagens a enviar para o equipamento configurado como coordenador através da sua interface de comunicação serie UART.

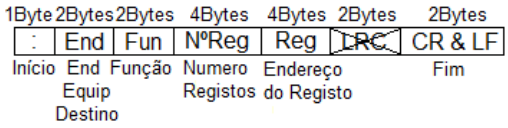


Figura A7.15: estrutura da mensagem a enviar (f.p)

Como é possível verificar pela imagem, o LRC está assinalado como anulado. A estrutura representada refere, tal como enunciado anteriormente, a mensagem a enviar para o equipamento coordenador, o qual após recebê-la irá reencaminhá-la para o respetivo dispositivo terminal possibilitando o retorno da informação pretendida. O valor do LRC na mensagem enviada pelo coordenador é por ele calculado e inserido antes do envio para o respetivo dispositivo terminal.

O campo função na configuração funcional descrita admite quatro valores distintos, sendo eles:

01 – Adquirir o estado de Saídas digitais;

02 – Adquirir o estado de Entradas digitais;

03 – Adquirir o valor de uma posição de memória (leitura ADC neste sistema);

05 – Ativar/Desativar uma saída digital;

Para facilitar a perceção da funcionalidade de Controlo e aquisição, a Figura A7.16 demonstra um exemplo desta, adquirindo e controlando estados de interfaces de dois equipamentos configurados como dispositivos terminais com endereços 0x02 e 0x03. O exemplo apresentado foi realizado através da conexão do equipamento coordenador a um computador.

Figura A7.16: funcionalidade de controlo e aquisição (f.p)

Como é possível ainda observar na Figura A7.16, as mensagens de resposta admitem uma estrutura diferente. De modo a possibilitar a compreensão das mensagens, a Figura A7.17 representa esquematicamente a estrutura das mensagens recebidas.

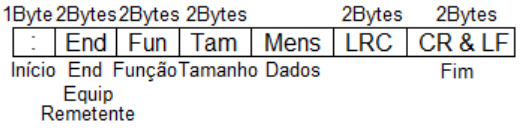


Figura A7.17: estrutura da mensagem recebida (f.p)

Com o intuito de representar o diálogo entre equipamentos nesta funcionalidade do sistema, a Figura A7.18 apresenta um diagrama de interação dos mesmos.

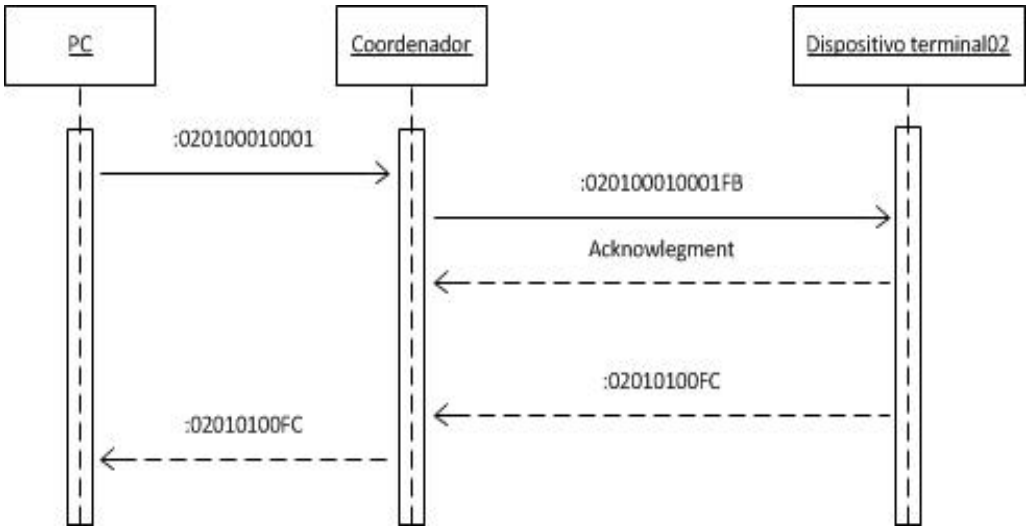


Figura A7.18: diagrama de interação da funcionalidade de controlo e aquisição (f.p)